Myndighetsdatalag

Slutbetänkande av
Informationshanteringsutredningen

Stockholm 2015

STATENS OFFENTLIGA UTREDNINGAR

SOU 2015:39

SOU och Ds kan köpas från Fritzes kundtjänst.
Beställningsadress: Fritzes kundtjänst, 106 47 Stockholm
Ordertelefon: 08-598 191 90
E-post: order.fritzes@nj.se
Webbplats: fritzes.se

För remissutsändningar av SOU och Ds svarar Fritzes Offentliga Publikationer
på uppdrag av Regeringskanslets förvaltningsavdelning.
Svara på remiss – hur och varför.
Statsrådsberedningen, SB PM 2003:2 (reviderad 2009-05-02)
En kort handledning för dem som ska svara på remiss. Häftet är gratis och kan laddas ner som pdf från eller beställas på regeringen.se/remiss.

Layout: Kommittéservice, Regeringskansliet.
Omslag: Elanders Sverige AB.
Tryck: Elanders Sverige AB, Stockholm 2015.

ISBN 978-91-38-24277-3
ISSN 0375-250X

Till statsrådet och chefen för Justitiedepartementet

Den 6 oktober 2011 bemyndigade regeringen chefen för Justitiedepartementet att tillkalla en särskild utredare med uppdrag att se över den s.k. registerlagstiftningen och vissa därmed sammanhängande frågor. Regeringen beslutade samtidigt om direktiv för utredningen (dir. 2011:11).

Till särskild utredare förordnades från och med den 25 oktober 2011 justitierådet Henrik Jermsten.

Utredningen har antagit namnet Informationshanteringsutredningen (Ju 2011:11).

I januari 2013 lämnades delbetänkandet Överskottsinformation vid direktåtkomst (SOU 2012:90).

Den 6 mars 2014 beslutade regeringen tilläggsdirektiv med förändrad inriktning avseende metoden för översynen m.m. (dir. 2014:31). Nya tilläggsdirektiv om viss förlängning av redovisningstiden beslutades den 20 november 2014 (dir. 2014:147).

Utredaren har biträtts av en sakkunnig, experter och ett sekretariat. Medverkande i den del av uppdraget som redovisas i detta betänkande anges på omstående sidor.

Härmed överlämnas slutbetänkandet Myndighetsdatalag (SOU 2015:39).

Till betänkandet fogas ett särskilt yttrande av experten Per Furberg.

Uppdraget är härmed slutfört.

Stockholm i april 2015

Henrik Jermsten

/Elisabet Reimers
Anna Tansjö

Förteckning över sakkunnig, experter och sekreterare som deltagit i utredningsarbetet fr.o.m. januari 2013.

(förordnade fr.o.m. den 16 januari 2012 om inget annat anges)

Sakkunnig

Eva Lenberg, rättschef, Utbildningsdepartementet

Experter

Maria Arnell, dåvarande rättssakkunnig, Justitiedepartementet (fr.o.m. 2013-01-12 t.o.m. 2013-07-31)
Malgorzata Drewniak, jurist, Lantmäteriet
Per Furberg, advokat, numera Advokataktiebolaget Per Furberg
Anneli Hagdahl, ämnessakkunnig, Näringsdepartementet (t.o.m. 2013-11-04)
Per Hultengård, chefsjurist, Tidningsutgivarna
Torbjörn Hörnfeldt, enhetschef, Riksarkivet
Linn Kempe, förvaltningsjurist, Bolagsverket, (med uppehåll fr.o.m. 2013-01-12 t.o.m. 2014-09-30)
Hans-Olof Lindblom, chefsjurist, Datainspektionen
Elisabet Reimers, kammarrättsråd, fr.o.m. 2015-02-01
Irene Reuterfors-Mattsson, förbundsjurist, Sveriges Kommuner och Landsting (t.o.m. 2013-12-31)
Svante Nygren, analytiker, Myndigheten för samhällsskydd och beredskap
Cecilia Magnusson Sjöberg, professor, Stockholms universitet
Nils Sjöblom, rättssakkunnig, Justitiedepartementet (fr.o.m. 2013-11-11)
Kjell-Åke Sjödin, områdesexpert, Transportstyrelsen
Per Trehörning, ombudsman, Svenska Journalistförbundet
Monika Vestin, dåvarande förvaltningsjurist, Bolagsverket (fr.o.m. 2013-01-12 t.o.m. 2014-09-30)
Mikael Westberg, numera chefsjurist, Pensionsmyndigheten, tidigare verksamhetsområdeschef, Försäkringskassan (fr.o.m. 2013-11-11)

Staffan Wikell, förbundsjurist, Sveriges Kommuner och Landsting
(fr.o.m. 2014-01-01)
Maria Östgren, rättslig expert, Skatteverket

Sekreterare

Katarina Dunnington, dåvarande kammarrättsassessor
(t.o.m. 2013-06-30)
Elisabet Reimers, kammarrättsråd,
(fr.o.m. 2013-10-01 t.o.m. 2015-01-31)
Anna Tansjö, rådman

Innehåll

Förkortningar m.m.

Förkortningar

BrB	brottsbalken
dataskyddsdirektivet	Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter
DIFS	Datainspektionens författningssamling
dir.	direktiv
dnr	diarienummer
Ds	Departementsserien
EU	Europeiska unionen
EU-domstolen	Europeiska unionens domstol/Europeiska gemenskapernas domstol
EU-fördraget	Fördraget om Europeiska unionen
Europadomstolen	Europeiska domstolen för de mänskliga rättigheterna
Europakonventionen	Europeiska konventionen den 4 november 1950 angående skydd för de mänskliga rättigheterna och de grundläggande friheterna
f.	följande sida/sidor
FL	förvaltningslagen (1986:223)

FPL	förvaltningsprocesslagen (1971:291)
HFD	Högsta förvaltningsdomstolens årsbok
JK	Justitiekanslern
Ju	Justitiedepartementet
JO	Riksdagens ombudsmän
KL	kommunallagen (1991:900)
kommissionen	Europeiska kommissionen
KU	konstitutionsutskottet
MSBFS	Myndigheten för samhällsskydd och beredskaps författningssamling
NJA	Nytt juridiskt arkiv, avdelning I
OSL	offentlighets- och sekretesslagen (2009:400)
prop.	regeringens proposition
PuF	personuppgiftsförordningen (1998:1191)
PuL	personuppgiftslagen (1998:204)
RA-FS	Riksarkivets författningssamling
RB	rättegångsbalken
RF	regeringsformen
RO	riksdagsordningen
RÅ	Regeringsrättens årsbok
SekrL	sekretesslagen (1980:100)
SFB	socialförsäkringsbalken
SkL	skadeståndslagen (1972:207)
skr.	regeringens skrivelse
SOU	Statens offentliga utredningar
TU	trafikutskottet
TF	tryckfrihetsförordningen

uppgiftsskyddsförordningen	Europeiska kommissionens förslag den 25 januari 2012 till Europaparlamentets och rådets förordning om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (allmän uppgiftsskyddsförordning)

Kortformer för viss citerad litteratur

Hellners/Malmqvist	Trygve Hellners, Bo Malmqvist, Förvaltningslagen. Med kommentarer, 31 maj 2010, Zeteo
Holmberg m.fl.	Erik Holmberg, Nils Stjernquist, Magnus Isberg, Marianne Eliason, Göran Regner, Grundlagarna. 1 januari 2012, Zeteo
Lenberg m.fl.	Eva Lenberg, Ulrika Geijer, Anna Tansjö, Offentlighets- och sekretesslagen. En kommentar, 2009, 1 juli 2014, Zeteo
Öman/Lindblom	Sören Öman, Hans-Olof Lindblom, Personuppgiftslagen. En kommentar, uppl. 4:1, 2011

Sammanfattning

Vårt uppdrag

I detta slutbetänkande redovisar vi vårt övergripande uppdrag att se över den s.k. registerlagstiftningen, ett rättsområde som omfattar ett stort antal sektors- eller myndighetsspecifika lagar och förordningar som kompletterar personuppgiftslagen (1998:204) och innehåller bestämmelser om statliga och kommunala myndigheters behandling av personuppgifter. Denna översyn ska ske genom att utreda förutsättningarna för att skapa en generell, enhetlig och – helt eller i vart fall delvis – samlad reglering för myndigheternas behandling av personuppgifter (dir. 2014:31). Den brottsbekämpande verksamheten ingår dock inte i vårt uppdrag.

Det kan inledningsvis påpekas att vårt uppdrag i huvudsak är ett lagtekniskt reformarbete med inriktning på att göra nu gällande rätt beträffande dataskydd tydligare på myndighetsområdet. Några betydande förändringar vad gäller om och hur myndigheter får behandla personuppgifter eller omprövningar av tidigare avvägningar mellan t.ex. effektivitetssträvanden och skyddet för enskildas personliga integritet ingår alltså inte i uppdraget.

Problembild

Vårt uppdrag har sin bakgrund i att det i olika sammanhang framförts kritik mot registerlagstiftningen för att vara ett svåröverblickbart och fragmenterat rättsområde med bristande enhetlighet i struktur och normtekniska lösningar samt med, i en del fall, otillräcklig anpassning till annan lagstiftning av central betydelse för myndigheternas informationshantering såsom tryckfrihetsförordningens bestämmelser om allmänna handlingar och offentlighets- och sekretesslagen (2009:400). Vi delar i stort denna problembild

och har kunnat konstatera att problemen skapar osäkerhet i tillämpningen, vilket bl.a. gör uppgiftsutbyte och annat samarbete mellan myndigheter onödigt komplicerat. Det försvårar också för enskilda registrerade och allmänheten att förstå vad som egentligen gäller för myndigheters informationshantering. Vidare är det ett problem i sig att registerlagar ofta behöver ändras till följd av att myndigheterna får nya uppgifter.

Ett ytterligare problem som vi identifierat är att den allmänna regleringen i personuppgiftslagen har utformats utan hänsyn till de särskilda förhållanden som gäller för myndigheters personuppgiftsbehandling. För myndigheter i allmänhet, dvs. inte bara för sådana som omfattas av särskild registerlagstiftning, präglas personuppgiftsbehandlingen av att den sker i verksamheter som är författningsreglerade, oftast i fråga om såväl vad som ska göras som hur det ska göras. Den informationshantering som verksamheten genererar styrs vidare av, utöver tidigare nämnda regelverk, annan central reglering, exempelvis förvaltningslagen (1986:223) och arkivlagen (1990:782) som alltså gäller utöver personuppgiftslagen. Detta förhållande innebär generellt sett en avgörande skillnad i jämförelse med personuppgiftsbehandling inom den enskilda sektorn.

Inledande ställningstaganden och utgångspunkter för en generell reglering

Mot bakgrund av bl.a. den beskrivna problembilden finns ett angeläget behov av förändringar i den reglering som rör personuppgiftsbehandling inom den offentliga sektorn. En samlad reglering i en lag om myndigheters behandling av personuppgifter gör det möjligt att åstadkomma ett tydligt regelverk som är lättare att tillämpa och bättre anpassat till övrig reglering av betydelse för myndigheters informationshantering. En sammanhållen lag ger också bättre förutsättningar för allmänhetens insyn och för enskilda registrerades möjligheter att göra gällande sina rättigheter enligt det dataskyddsrättsliga regelverket. Till bilden hör vidare att en samlad reglering är mer ändamålsenlig för att möta den förändring som förväntas ske på det unionsrättsliga området genom en EU-förordning om allmänt uppgiftsskydd som ska ersätta det s.k. dataskyddsdirektivet.

Vi föreslår därför en ny lag – myndighetsdatalagen – som företer likheter med förekommande registerförfattningar men som innehåller bestämmelser som kan gälla generellt för alla statliga och kommunala myndigheters personuppgiftsbehandling frånsett den brottsbekämpande sektorn.

Vårt förslag till ny lag har arbetats fram utifrån bl.a. följande utgångspunkter.

Regleringen bör utformas som en renodlad persondataskyddsreglering som bara tar sikte på frågor om skydd för personuppgifter som uppstår i myndigheternas elektroniska informationshantering, vilken är en integrerad del av myndigheternas verksamheter på alla nivåer. Bestämmelserna i den nya lagen ska alltså inte i något avseende syfta till att reglera en myndighets sakverksamhet.

Till den nya lagen ska det kunna finnas bilagor och en anslutande förordning. Efter hand som behov av sektors- eller myndighetsspecifika särregler uppstår kan sådana tas in i en systematiskt ordnad reglering som kompletterar den nya lagen. På så sätt uppnås ett sammanhållet ramverk med enhetligt utformad reglering både vad avser förhållanden som kan regleras generellt och förhållanden där fortsatta särregler – utifrån närmare avvägningar mellan integritetsintressen och t.ex. effektivitetshänsyn på området i fråga – behöver finnas. Det är dock vår bedömning att behovet av fortsatt särreglering kommer att minska betydligt.

Det är vår uppfattning att den särreglering av persondataskyddsfrågor som även fortsättningsvis behöver finnas oftast ska kunna ges i förordning, vilket förenklar regelgivningen och underlättar nödvändiga förändringar vid ändringar i myndigheternas uppgifter m.m. Normgivningsreglerna i regeringsformen kräver normalt inte lagform för reglering av detta slag. Det sagda utesluter givetvis inte att lagnivå ibland krävs eller i vart fall framstår som lämplig av hänsyn till skyddet för enskildas integritet.

Den nya lagen utesluter inte att det även fortsättningsvis för vissa myndigheter eller verksamheter kan komma att bedömas vara mera lämpligt från lagtekniska, systematiska eller andra synpunkter med särreglering i separat författning som gäller utöver den nya lagen, på motsvarande sätt som många registerlagar i dag förhåller sig till personuppgiftslagen.

Renodlade registerförfattningar om inrättandet och förandet av specifika register utgör ett slags verksamhetsreglering som även i

fortsättningen bör regleras i särskild ordning, dvs. utanför den samlade regleringen.

Eftersom en kommande EU-förordnings närmare innehåll av betydelse på myndighetsområdet – liksom ikraftträdandetidpunkten – fortfarande är i hög grad oklart bör den nya lagen vara anpassad till gällande rätt på persondataskyddsområdet, dvs. till personuppgiftslagen.

Om myndighetsdatalagens innehåll

Lagens syfte och tillämpningsområde

Lagens syfte ska vara att dels ge myndigheter möjlighet att behandla personuppgifter på ett ändamålsenligt sätt i deras verksamheter, dels skydda människor mot att deras personliga integritet kränks vid sådan behandling.

Lagen ska i princip tillämpas av alla statliga och kommunala myndigheter vid behandling av personuppgifter som är helt eller delvis automatiserad eller avser manuell registerföring.

Vissa verksamheter undantas dock från lagens tillämpningsområde nämligen 1) en myndighets administrativa verksamhet, 2) en myndighets verksamhet som personuppgiftsbiträde och 3) sådan verksamhet som bedrivs av behöriga myndigheter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller beivra brott eller verkställa straffrättsliga påföljder.

Förhållandet till avvikande bestämmelser i annan lag eller förordning och till personuppgiftslagen

Lagen ska – med undantag för personuppgiftslagen och bestämmelser som meddelats med stöd av den lagen – vara subsidiär i förhållande till bestämmelser i annan lag eller förordning som avviker från lagens bestämmelser. Lagen har vidare konstruerats på det sättet att den gäller i stället för personuppgiftslagen, dock att det särskilt hänvisas till vissa bestämmelser i personuppgiftslagen som ska tillämpas på motsvarande sätt vid myndigheters behandling av personuppgifter enligt den nya lagen. Enligt dessa hänvisningar ska alltså personuppgiftslagens bestämmelser om defini-

tioner (3 §), förhållandet till handlingsoffentligheten och arkivlagstiftningen (8 §) och grundläggande krav på behandlingen (9 §) gälla. Dessutom hänvisas till personuppgiftslagens förbud mot behandling av sådana personuppgifter som definieras som känsliga (13 §) samt till undantagen från förbudet vid behandling med den registrerades uttryckliga samtycke (15 §), i vissa fall av nödvändig behandling (16 §), för hälso- och sjukvårdsändamål (18 §) samt för forsknings- eller statistikändamål (19 §). Vidare ska, i huvudsak, personuppgiftslagens bestämmelser om information som ska lämnas till den registrerade – dels i samband med att uppgifter samlas in, dels på begäran – tillämpas (23, 25 och 26 §) liksom bestämmelserna om överföring till tredjeland (33–35 §§) och om personuppgiftsombud (38 och 40 §§). Slutligen ska personuppgiftslagens bestämmelser om skadestånd (48 §) tillämpas på motsvarande sätt, dvs. en personuppgiftsanvarig myndighets skyldighet att följa bestämmelserna i såväl den nya lagen som bestämmelser i personuppgiftslagen som den nya lagen hänvisar till ska vara skadeståndssanktionerad.

Den s.k. missbruksregeln i 5 a § PuL föreslås inte vara tillämplig på myndighetsområdet och något liknande generellt undantag från personuppgiftslagens s.k. hanteringsregler införs inte i den nya lagen. Vår analys av den frågan har resulterat i bedömningen att ett sådant generellt undantag från hanteringsreglerna såvitt avser behandling av personuppgifter i s.k. ostrukturerat material varken behövs på myndighetsområdet eller framstår som en rättsligt befogad begränsning i förhållande till dataskyddsdirektivets krav. Endast i ett avseende innehåller den nya lagen ett motsvarande undantag, nämligen i fråga om information till den registrerade som ska lämnas efter ansökan (26 § PuL). Sådan information behöver inte omfatta personuppgifter som behandlas i ostrukturerat material.

Personuppgiftsansvar och personuppgiftsbiträden

I den nya lagen införs en generell regel som innebär att en myndighet alltid är personuppgiftsansvarig för den behandling som myndigheten utför. Vidare klargörs att personuppgiftsansvaret även omfattar sådan behandling som en mottagande myndighet utför när denna via direktåtkomst hos en annan myndighet eller enskild i

ett enskilt fall genom en överföring faktiskt behandlar en tillgänglig personuppgift.

Det som föreskrivs i personuppgiftslagen om att ett personuppgiftsbiträde eller den som arbetar under biträdets ledning bara får behandla personuppgifter i enlighet med den personuppgiftsansvariges instruktioner ska gälla genom att motsvarande bestämmelser tas in i den nya lagen. Detsamma gäller kravet på att det ska finnas ett skriftligt avtal med personuppgiftsbiträdet liksom kraven på vad avtalet ska innehålla. Utöver detta införs ett krav på att avtalet ska innehålla dokumentation om den personuppgiftsansvariga myndighetens instruktioner till biträdet samt ett förbud mot att biträdet anlitar ett annat biträde, ett s.k. underbiträde, utan godkännande från den personuppgiftsansvariga myndigheten. Samma villkor om avtal och instruktioner ska gälla för ett sådant underbiträde.

När behandling kan tillåtas

I lagen införs en samlad rättslig grund för behandling av personuppgifter som ersätter bestämmelserna i 10 § a–f PuL om när behandling av personuppgifter är tillåten oberoende av den registrerades samtycke. Bestämmelsen innebär att en myndighet får behandla personuppgifter om det är nödvändigt för att myndigheten ska kunna utföra sin verksamhet. Vilken verksamhet en myndighet har som uppgift eller fått befogenhet att utföra framgår av författningsreglering eller särskilda beslut i regleringsbrev m.m.

Någon begränsning av för vilka ändamål som myndigheter får behandla personuppgifter föreslås inte i den nya lagen. Därmed blir huvudregeln att det är den personuppgiftsansvariga myndigheten som, inom ramen för sitt uppdrag, har att närmare specificera för vilket eller vilka ändamål personuppgifter behandlas i verksamheten. Dessa ändamål måste uppfylla det grundläggande kravet på att vara särskilda och uttryckligt angivna redan vid insamlingen. Även framöver kan det dock på vissa områden, t.ex. i fråga om vissa särskilt integritetskänsliga informationssamlingar, finnas anledning att genom särskilda föreskrifter i lag eller förordning om ändamålsbegränsningar ange ramar för myndigheters personuppgiftsbehandling. Sådana föreskrifter kan tas in i den till lagen anslutande

förordningen alternativt, för det fall lagnivå undantagsvis anses nödvändig eller lämplig, i bilaga till lagen.

Särskilda kategorier av personuppgifter

Ytterligare undantag från förbudet att behandla känsliga personuppgifter

Utöver vad som följer av 15, 16, 18 och 19 §§ PuL tillåts myndigheter att behandla känsliga personuppgifter om uppgifterna har lämnats i ett ärende eller är nödvändiga för handläggning av det. I annan verksamhet får känsliga personuppgifter behandlas endast i löpande text. Regeringen eller den myndighet som regeringen bestämmer bemyndigas att medge ytterligare undantag, om det behövs med hänsyn till ett viktigt allmänt intresse.

Personnummer i beslut m.m.

Enligt en särskild bestämmelse i lagen får personnummer och samordningsnummer tas in i en myndighets beslut endast om beslutet rör en enskilds identitet eller motsvarande personliga förhållanden. Sådana uppgifter får också tas in i ett beslut om det är nödvändigt för att beslutet ska kunna verkställas eller om det krävs med hänsyn till beslutande myndighets behov av identifieringsuppgifter. Vid övrig behandling, dvs. som inte avser beslut, sätter de grundläggande kraven enligt 9 § PuL gränserna för i vilken omfattning personnummer eller samordningsnummer får behandlas.

Sökförbud

Enligt en bestämmelse i lagen ska gälla att myndigheter vid en sökning får som sökbegrepp använda uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening eller uppgifter som rör hälsa eller sexualliv endast i den utsträckning som det finns särskilt författningsstöd för det. Sådant stöd kan anges genom föreskrifter som tas in i bilaga till lagen, i annan lag eller i förordning. Därmed gäller alltså som huvudregel ett generellt förbud för myndigheter

att som sökbegrepp använda uppgifter som leder till att känsliga personuppgifter sammanställs. Förbudet gäller såväl sökningar i myndighetens egna informationssamlingar som i fråga om personuppgifter som myndigheten har tillgång till genom direktåtkomst och har betydelse för vilka sammanställningar, s.k. potentiella handlingar, som enligt 2 kap. 3 § andra stycket TF anses vara förvarade allmänna handlingar hos myndigheten. I bestämmelsen klargörs dock att förbudet inte gäller vid sökning i en viss handling eller i ett visst ärende. Regeringen bemyndigas att meddela föreskrifter om sökbegränsningar i fråga om andra uppgiftskategorier än de som förbjuds i lagen.

Säkerhet till skydd för personuppgifter

Skyldigheterna i fråga om säkerhetsåtgärder och lämplig säkerhetsnivå framgår genom en bestämmelse i lagen som ersätter 31 § första stycket PuL. Enligt bestämmelsen är myndigheter skyldiga att vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna ska åstadkomma en lämplig säkerhetsnivå som ska bestämmas utifrån de risker som behandlingen medför och personuppgifternas karaktär. Vidare anges att säkerhetsarbetet ska omfatta förebyggande, löpande och uppföljande åtgärder samt att säkerhetsarbetet ska ske med beaktande av andra föreskrifter om informationssäkerhet i lag eller annan författning. Härmed klargörs den nära kopplingen mellan den personuppgiftsskyddsrättsliga regleringen av säkerheten för personuppgifter och det vidare regelverk om informationssäkerhet som myndigheterna också är skyldiga att följa.

Vidare föreskrivs en skyldighet för varje myndighet att se till att anställda bara ges tillgång till personuppgifter utifrån vad som krävs för arbetsuppgifterna. Detta ska gälla i fråga om såväl personuppgifter i myndighetens egna informationssamlingar som personuppgifter som myndigheten får tillgång till genom direktåtkomst.

Elektroniskt utlämnande

Åtskillnaden mellan direktåtkomst och annat utlämnande i elektronisk form

En särskild delfråga i utredningsuppdraget har varit att överväga om det finns anledning att behålla en rättslig åtskillnad mellan olika former av elektroniskt utlämnande av personuppgifter eller om denna åtskillnad bör utmönstras. Vad detta handlar om är den i registerförfattningar vanliga åtskillnaden mellan regler som gäller för direktåtkomst och utlämnande på medium för automatiserad behandling – eller som vi kallar det – annat utlämnande i elektronisk form. Som regel föreskrivs betydligt snävare förutsättningar för utlämnande genom direktåtkomst.

Vi har ingående analyserat denna fråga och kommit till slutsatsen att en begreppsmässig skillnad mellan å ena sidan direktåtkomst och å andra sidan annat utlämnande i elektronisk form bör behållas. Direktåtkomst innebär rättsligt sett att gränsen mellan de uppgiftsutbytande myndigheterna i viss omfattning tas bort, vilket inte är konsekvensen av ett annat elektroniskt utlämnande. Hur den mottagande myndigheten väljer att använda direktåtkomsten har den utlämnande myndigheten inte någon befogenhet att påverka, eftersom de handlingar som omfattas av åtkomsten redan har lämnats ut. Korresponderande sekretessfrågor måste därför vara lösta på förhand liksom behov av sökbegränsningar hos den mottagande myndigheten, vilket kan medföra krav på lagstiftningsåtgärder. Både principiella och rättsliga skäl talar därför för att en åtskillnad görs. Direktåtkomst medför också krav på förberedande analyser och åtgärder ur verksamhets- och personuppgiftsansvarsperspektiv, bl.a. i fråga om tekniskt genomförande och säkerhet. Varken den tekniska utvecklingen eller effektivitetsvinster och integritetsrisker som kan förknippas med olika åtkomstmetoder utgör vidare skäl för att utmönstra den begreppsmässiga åtskillnaden. Om en åtskillnad inte görs mellan direktåtkomst och annat elektroniskt utlämnande finns en risk för att de särskilda frågor om skydd och ansvarsfördelning, som sammanhänger med att myndigheternas gränser öppnas upp genom en direktåtkomst, inte får tillräcklig uppmärksamhet. En väl genomtänkt och genomförd direktåtkomst behöver emellertid inte innebära större risker för den

enskildes integritet än annat elektroniskt utlämnande av personuppgifter.

Ett sådant utlämnande i elektronisk form som inte är direktåtkomst innebär – oavsett på vilket sätt det sker – inte i något fall att myndigheternas verksamhet rättsligt sett blandas samman. Något behov av att rättsligt skilja olika sådana former åt finns därför inte. Skilda sätt att elektroniskt förmedla uppgifter från en myndighet till en annan kan dock innebära att olika slags säkerhetsrisker behöver beaktas.

I konsekvens med vår bedömning i dessa frågor innehåller den nya lagen olika reglering för direktåtkomst respektive annat utlämnande i elektronisk form.

Direktåtkomst

Med begreppet direktåtkomst avses, liksom hittills, en sådan teknisk tillgång till upptagningar hos annan som avses i 2 kap. 3 § andra stycket TF. Enligt den nya lagen gäller inte något allmänt krav på författningsstöd för att direktåtkomst ska kunna förekomma. Däremot föreskriver den nya lagen att direktåtkomst till sekretessreglerade personuppgifter ska ha stöd i lag eller förordning. Undantag från kravet på författningsstöd såvitt gäller sekretessreglerade personuppgifter gäller dock för direktåtkomst 1) som medges den registrerade eller dennes ombud och som tar sikte på uppgifter som hänför sig till den registrerade, 2) som medges till uppgifter som är sekretessreglerade enligt 21 kap. 7 § OSL, 3) som medges ett personuppgiftsbiträde och 4) som medges en myndighet endast för sådan teknisk bearbetning eller teknisk lagring som avses i 2 kap. 10 § TF för den utlämnande myndighetens räkning.

Överenskommelser vid direktåtkomst m.m.

I linje med vår bedömning angående varför direktåtkomst kräver särskilda överväganden och åtgärder föreskrivs i den nya lagen att en utlämnande myndighet ska göra en risk- och sårbarhetsanalys innan myndigheten medger en annan myndighet eller enskild aktör direktåtkomst till personuppgifter. Vidare ska myndigheten komma överens med mottagaren hur behövligt skydd för personuppgift-

erna ska säkerställas. Av överenskommelsen ska också framgå hur utövandet av de skyldigheter som personansvaret innefattar ska ske. Motsvarande ska gälla vid andra former av informationsutbyten som innebär behandling av personuppgifter i gemensamma eller annars integrerade informationssystem. Överenskommelsen i fråga om personuppgiftsansvarets utövande ska inte vara bindande utåt sett utan i första hand syfta till att klargöra ansvarsförhållandena mellan samarbetsparterna. Kravet på risk- och sårbarhetsanalyser och överenskommelser omfattar direktåtkomst m.m. i fråga om både offentliga och sekretessreglerade personuppgifter.

Sökbegränsning vid direktåtkomst

En särskild delfråga i uppdraget har varit att ta ställning till om sökförbud för en utlämnande myndighet bör gälla vid direktåtkomst för en mottagande myndighet. Vi har dock bedömt att det inte är ändamålsenligt att motverka eventuella risker för enskildas integritet i samband med direktåtkomst genom att föreskriva att samma sökbegränsningar alltid ska gälla för såväl den utlämnande myndigheten som den mottagande myndigheten. Det kan leda till att enskildas integritet inte skyddas i tillräcklig utsträckning, men också att en mottagande myndighets berättigade behov av att använda sig av de uppgifter som blir åtkomliga genom direktåtkomst inte kan tillgodoses. Enskildas integritet bör i stället skyddas genom att en direktåtkomst inte medges förrän noggranna överväganden har gjorts beträffande den mottagande myndighetens användning av direktåtkomsten, bl.a. beträffande vilka sökbegränsningar som den ska iaktta.

Annat utlämnande i elektronisk form

Enligt vår bedömning saknas det skäl för att införa ett grundläggande krav på att utlämnanden av personuppgifter i elektronisk form ska ha stöd i författning för att vara tillåtet. Vi har inte heller funnit skäl att generellt begränsa myndigheters möjlighet att lämna ut personuppgifter till andra myndigheter eller enskilda i elektronisk form. När det gäller utlämnanden till enskilda innehåller emellertid den nya lagen en bestämmelse som erinrar om att om en person-

uppgift får lämnas ut till en enskild, kan det ske i elektronisk form om det inte är olämpligt med hänsyn till skyddet för personuppgiften. Därmed erinras myndigheterna om att det ankommer på dem att först göra en prövning av om ett utlämnande, oavsett form, av personuppgifter är tillåtet. Om så är fallet, är utgångspunkten att det kan ske i elektronisk form.

Överföring till tredjeland

Den nya lagen innehåller två undantag från förbudet mot överföring av personuppgifter till tredjeland som saknar adekvat skyddsnivå – utöver de som följer av 34 och 35 §§ PuL – nämligen om överföringen krävs för myndighetens handläggning av ett visst ärende eller om överföringen är nödvändig för att fullgöra en uppgiftsskyldighet som följer av lag eller förordning eller avtal med annan stat eller mellanfolklig organisation som Sverige har tillträtt eller annars är förpliktat att följa.

Förteckning över behandlingar

Myndigheters behandling av personuppgifter enligt den nya lagen ska inte omfattas av anmälningsskyldighet till tillsynsmyndigheten. Varje myndighet ska i stället föra en förteckning över de behandlingar som utförs med stöd av lagen. Förteckningen avses innehålla motsvarande uppgifter som en anmälan till tillsynsmyndigheten enligt 36 § PuL skulle ha innehållit. Närmare föreskrifter om förteckningens innehåll meddelas av regeringen eller myndighet som regeringen bestämmer.

Korrigering av felaktig eller otillåten behandling

Personuppgiftslagens bestämmelser om rättelse m.m. (28 §) är ett exempel på bestämmelser som utformats utan hänsyn till de särskilda förhållanden som gäller för myndigeters informationshantering. I den nya lagen finns därför en mer ändamålsenligt utformad reglering rörande korrigering genom dels en bestämmelse som tar sikte på en myndighets skyldighet att rätta felaktiga eller

ofullständiga uppgifter, dels en bestämmelse som tar sikte på skyldigheten att korrigera en behandling som av andra skäl inte är tillåten enligt lagen.

Den förstnämnda bestämmelsen föreskriver en skyldighet för en myndighet att på begäran av den registrerade rätta eller komplettera en personuppgift som rör den registrerade, om uppgiften är felaktig eller ofullständig till följd av en åtgärd som inte har sin grund i myndighetens eller någons annans bedömning, exempelvis ett förbiseendefel eller ett tekniskt fel.

Den andra bestämmelsen föreskriver att en personuppgift på begäran av den registrerade ska avskiljas från fortsatt behandling och inte lämnas ut till en enskild annat än med stöd av 2 kap. TF eller utplånas, om uppgiften rör honom eller henne och inte får behandlas enligt den nya lagen eller föreskrifter som har meddelats med stöd av den. Bestämmelsen tar sikte på korrigeringar som begärs av en registrerad och som innebär att myndigheten behöver göra en bedömning av om behandlingen är tillåten, exempelvis för att den registrerade gör gällande att uppgifter behandlas som inte är relevanta för ändamålet med behandlingen i fråga. Rätten att begära en korrigering av nu nämnt slag ska inte gälla personuppgifter i en myndighets beslut.

Tillsynsmyndighetens befogenheter

Enligt den nya lagen ska tillsynsmyndighetens åtgärder i form påpekanden eller liknande förfaranden som inte har tvingande karaktär användas endast i förebyggande syfte, dvs. om tillsynsmyndigheten konstaterat att en myndighet kan komma att behandla personuppgifter på ett olagligt sätt, och inte då det har konstaterats att en behandling av personuppgifter utförs på ett otillåtet sätt.

Vidare föreskrivs att tillsynsmyndigheten ska kunna förelägga en myndighet att uppfylla sina skyldigheter om myndigheten inte uppfyller de krav som följer av den nya lagen eller föreskrifter som meddelats med stöd av den. I föreläggandet ska anges vad tillsynsmyndigheten anser är nödvändigt för att avhjälpa de påtalade bristerna.

Tillsynsmyndigheten ska också ha befogenhet att förbjuda en myndighet att fortsätta en behandling av personuppgifter på något

annat sätt än att uppgifterna lagras. Ett sådant beslut förutsätter att myndigheten allvarligt brister i sin skyldighet att uppfylla de krav som gäller för behandlingen. Ett beslut om förbud gäller omedelbart.

Någon möjlighet för tillsynsmyndigheten att besluta om vite har inte införts i lagen.

I övrigt finns bestämmelser som motsvarar dels 43 § PuL om vilka befogenheter tillsynsmyndighetens har för att undersöka om en myndighet behandlar personuppgifter på ett tillåtet sätt, dels 47 § PuL om tillsynsmyndighetens möjlighet att hos förvaltningsrätten ansöka om utplåning av personuppgifter som har behandlats på ett olagligt sätt.

Överklagande

I lagen finns bestämmelser om överklagande av tillsynsmyndighetens respektive personuppgiftsansvariga myndigheters beslut som i princip motsvarar personuppgiftslagens överklagandebestämmelser (51–53 §§ PuL).

Sekretessfrågor

I 10 kap. OSL föreslås införas en generellt sekretessbrytande bestämmelse som innebär att föreskrifter i lag eller förordning om direktåtkomst för myndigheter i sig får en sekretessbrytande effekt. Därigenom kommer det inte längre att behövas särskilda sekretessbrytande bestämmelser för att möjliggöra direktåtkomst enligt den ordning som i dag vanligtvis tillämpas. För att en bestämmelse om direktåtkomst ska ha sekretessbrytande effekt enligt den nya bestämmelsen krävs dock att den har en sådan konkretion att det framgår i fråga om vilka uppgifter sekretessen bryts. Den sekretessbrytande bestämmelsen omfattar inte direktåtkomst som medges utländska myndigheter eller enskilda.

Vi har som en särskild delfråga haft att överväga om det finns anledning att ändra 6 kap. 5 § OSL – som föreskriver en grundläggande skyldighet att på begäran lämna uppgifter till andra myndigheter – för att den ska stå i bättre överensstämmelse med användningsbegränsningar som kan förekomma i samband med internationella åtaganden. Vi har dock vid vår analys av frågan inte

funnit något tillräckligt stort praktiskt behov av en sådan ändring. Vi har därför inte föreslagit någon ändring i 6 kap. 5 § OSL.

Konsekvenser

Införandet av en samlad lag med anslutande reglering i bilaga eller förordning är ett långsiktigt arbete. Regleringen kan inte i ett slag ersätta befintliga registerförfattningar vid införandet. Syftet är emellertid att ett antal registerförfattningar efter hand ska kunna upphävas eller i vart fall förenklas betydligt. Eventuella kvarstående behov av särreglering ska vidare kunna infogas i den samlade regleringen. Det kräver emellertid närmare analyser och avvägningar angående behovet av fortsatta särregler på olika områden och på vilken normnivå dessa särregler i förekommande fall bör ges.

Initialt kommer därför lagen att vid ikraftträdandet gälla fullt ut bara för de myndigheter eller i de verksamheter som då endast behandlar personuppgifter med stöd av personuppgiftslagen. Detta innebär en viss omställning för dessa myndigheter. Vi bedömer dock att denna omställning inte är större eller kräver mer anpassningar än att den kan mötas med en väl tilltagen tid för ikraftträdandet och ett fåtal övergångsbestämmelser. Enligt vårt förslag bör den nya lagen träda i kraft den 1 januari 2017.

När den samlade regleringen väl är genomförd även beträffande översynen av de nuvarande registerförfattningarna bedömer vi att den samlade regelmassan kommer att minska betydligt. Genom att särreglering i fortsättningen utformas enhetligt och samordnat utifrån en gemensam systematik underlättas samarbete över myndighetsgränser. Flexibiliteten i regleringen ökar vidare genom vår ambition att fler frågor ska regleras i förordning. En på detta sätt samlad och därmed mer enhetlig och tydligare reglering kommer också att vara till gagn för offentlighet och insyn och ökar förutsättningarna att anpassa offentlighetsprincipen till moderna tekniska kommunikationsformer. Anpassningen till en kommande uppgiftsskyddsförordning underlättas också, då vad som hittills är känt om förhandlingarna inom unionen tyder på att den samlade regleringen utan alltför genomgripande förändringar kan anpassas till att utgöra ett komplement till förordningen.

1 Författningsförslag

1.1 Förslag till myndighetsdatalag

Härigenom föreskrivs följande.

Lagens syfte och tillämpningsområde

1 § Syftet med denna lag är att ge myndigheter möjligheter att behandla personuppgifter på ett ändamålsenligt sätt i deras verksamheter och att skydda människor mot att deras personliga integritet kränks vid sådan behandling.

2 § Denna lag gäller vid myndigheters behandling av personuppgifter.

Lagen gäller om behandlingen är helt eller delvis automatiserad eller om personuppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

3 § Lagen ska inte tillämpas vid behandling av personuppgifter i

1. en myndighets administrativa verksamhet,
2. en myndighets verksamhet som personuppgiftsbiträde, eller
3. den verksamhet som bedrivs av behöriga myndigheter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller beivra brott eller verkställa straffrättsliga påföljder.

Förhållandet till annan författning

4 § Om det i en annan lag eller förordning än som avses i 5 § finns bestämmelser som avviker från denna lag, ska de bestämmelserna gälla.

5 § Om inte annat anges i 6 § gäller denna lag i stället för personuppgiftslagen (1998:204) eller föreskrifter som meddelats i anslutning till den lagen.

6 § Följande bestämmelser i personuppgiftslagen (1998:204) ska tillämpas på motsvarande sätt när personuppgifter behandlas enligt denna lag eller föreskrifter som meddelats med stöd av den:

1. 3 § om definitioner,
2. 8 § om förhållandet till offentlighetsprincipen m.m.,
3. 9 § om grundläggande krav på behandlingen,
4. 13, 15, 16, 18 och 19 §§ om känsliga personuppgifter,
5. 23 och 25 §§ om information till den registrerade som ska lämnas självmant,
6. 26 § om information till den registrerade som ska lämnas efter ansökan,
7. 33–35 §§ om överföring av personuppgifter till tredjeland,
8. 38 och 40 §§ om personuppgiftsombud, och
9. 48 § om skadestånd.

I 23 § finns bestämmelser om undantag från informationsskyldigheten enligt första stycket 5 och 6.

Personuppgiftsansvar

7 § En myndighet är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför.

Personuppgiftsansvaret enligt första stycket omfattar även behandling som en myndighet utför genom direktåtkomst till personuppgifter hos en annan myndighet eller enskild.

När behandling kan tillåtas

8 § Personuppgifter får behandlas om det är nödvändigt för att en myndighet ska kunna utföra sin verksamhet.

9 § Behandling som är tillåten enligt denna lag eller föreskrifter som meddelats med stöd av den får utföras även om den registrerade motsätter sig behandlingen.

Särskilda kategorier av personuppgifter

10 § Utöver vad som följer av 15, 16, 18 och 19 §§ personuppgiftslagen (1998:204) får känsliga personuppgifter behandlas om uppgifterna har lämnats i ett ärende eller är nödvändiga för handläggning av det eller om uppgifterna behandlas endast i löpande text.

11 § Personnummer eller samordningsnummer får tas in i ett beslut endast om beslutet rör en enskilds identitet eller motsvarande personliga förhållanden, det är nödvändigt för att beslutet ska kunna verkställas eller det krävs med hänsyn till beslutande myndighets behov av identifieringsuppgifter.

Sökförbud

12 § Uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening liksom uppgifter som rör hälsa eller sexualliv får användas som sökbegrepp endast om det är tillåtet enligt föreskrifter som tagits in i bilaga till denna lag eller i annan lag eller förordning.

Vad som sägs i första stycket gäller inte vid en sökning i en viss handling eller i ett visst ärende.

Elektroniskt utlämnande

Direktåtkomst

13 § Direktåtkomst till personuppgifter som är sekretessreglerade är tillåten endast i den utsträckning som anges i bilaga till denna lag eller i annan lag eller förordning. Med sekretessreglerade uppgifter avses detsamma som i offentlighets- och sekretesslagen (2009:400).

Vad som sägs i första stycket gäller inte direktåtkomst som medges

1. den registrerade eller dennes ombud till uppgifter som hänför sig till den registrerade,
2. till personuppgifter som är sekretessreglerade enligt 21 kap. 7 § offentlighets- och sekretesslagen,
3. ett personuppgiftsbiträde, eller
4. en myndighet endast för sådan teknisk bearbetning eller teknisk lagring som avses i 2 kap. 10 § första stycket tryckfrihetsförordningen för den utlämnande myndighetens räkning.

14 § Innan en myndighet medger direktåtkomst till personuppgifter ska myndigheten göra en risk- och sårbarhetsanalys och komma överens med mottagaren av personuppgifterna hur skyddet för personuppgifterna ska säkerställas. Av överenskommelsen ska också framgå hur utövandet av de skyldigheter som personuppgiftsansvaret innefattar ska ske.

Vad som sägs i första stycket ska i tillämpliga delar även gälla då en myndighet på annat sätt än genom direktåtkomst samarbetar med andra myndigheter eller enskilda på sätt som innebär behandling av personuppgifter i gemensamma eller annars integrerade informationssystem.

Annat utlämnande i elektronisk form

15 § Får en personuppgift lämnas ut till en enskild, kan det ske i elektronisk form om det inte är olämpligt med hänsyn till skyddet för personuppgiften.

Överföring till tredjeland

16 § Utöver vad som följer av 34 § personuppgiftslagen (1998:204) eller av föreskrifter eller beslut som meddelats med stöd av 35 § samma lag får personuppgifter överföras till tredjeland som saknar adekvat skyddsnivå, om

1. överföringen krävs för handläggningen av ett visst ärende, eller
2. överföringen är nödvändig för att fullgöra en uppgiftsskyldighet som följer av lag eller förordning eller avtal med annan stat eller

mellanfolklig organisation som Sverige har tillträtt eller annars är förpliktat att följa.

Säkerhet vid behandlingen

17 § En myndighet ska vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder för att skydda de personuppgifter som behandlas. Säkerhetsarbetet ska omfatta förebyggande, löpande och uppföljande åtgärder samt åstadkomma en lämplig säkerhetsnivå i förhållande till de risker som behandlingen medför och karaktären hos de uppgifter som ska skyddas. Vid utformningen av säkerhetsåtgärderna ska myndigheten även beakta bestämmelser om informationssäkerhet i annan författning som gäller för myndigheten.

18 § Tillgången till personuppgifter ska begränsas till vad varje anställd behöver för att kunna fullgöra sina arbetsuppgifter.

Personuppgiftsbiträde

19 § Ett personuppgiftsbiträde eller den som arbetar under biträdets ledning får behandla personuppgifter bara i enlighet med instruktioner från den personuppgiftsansvariga myndigheten. Detta gäller även för biträden som anlitats av ett personuppgiftsbiträde.

20 § När en myndighet anlitar ett personuppgiftsbiträde, ska myndigheten förvissa sig om att biträdet

1. ser till att personuppgifter behandlas bara i enlighet med instruktioner från myndigheten,
2. kan genomföra de säkerhetsåtgärder som avses i 17 § och som måste vidtas till skydd för de personuppgifter som biträdet behandlar,
3. fortlöpande vidtar säkerhetsåtgärderna, och
4. inte anlitar annat biträde utan godkännande från myndigheten.

21 § Det ska finnas ett skriftligt avtal om personuppgiftsbiträdets behandling av personuppgifter för myndighetens räkning. Avtalet ska innehålla instruktioner och villkor om personuppgiftsbiträdets

skyldigheter i frågor som avses i 19 och 20 §§. Motsvarande avtal ska finnas med ett biträde som anlitats av ett personuppgiftsbiträde.

Förteckning över behandlingar

22 § En myndighet ska föra en förteckning över de behandlingar som myndigheten utför med stöd av denna lag.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela närmare föreskrifter om vilka uppgifter en sådan förteckning ska innehålla.

Undantag från informationsskyldigheten

23 § Bestämmelserna i 23, 25 och 26 §§ personuppgiftslagen (1998:204) ska inte tillämpas i den utsträckning som en uppgift inte får lämnas ut till den registrerade på grund av sekretess enligt offentlighets- och sekretesslagen (2009:400) eller föreskrifter som meddelats med stöd av den lagen.

Bestämmelserna i 26 § personuppgiftslagen behöver inte tillämpas vid behandling av personuppgifter som inte ingår i eller är avsedda att ingå i en samling av personuppgifter som har strukturerats för att påtagligt underlätta sökning efter eller sammanställning av personuppgifter.

Korrigering av felaktiga personuppgifter eller annars otillåten behandling

24 § En personuppgift ska på begäran av den registrerade rättas eller kompletteras om uppgiften rör honom eller henne och den är felaktig eller ofullständig till följd av en åtgärd som inte har sin grund i myndighetens eller någon annans bedömning.

25§ En personuppgift ska på begäran av den registrerade avskiljas från fortsatt behandling och inte lämnas ut till en enskild annat än med stöd av 2 kap. tryckfrihetsförordningen eller utplånas, om uppgiften rör honom eller henne och den inte får behandlas enligt denna lag.

Vad som sägs i första stycket gäller inte personuppgifter i ett beslut.

Tillsynsmyndighetens befogenheter

26 § Tillsynsmyndigheten har rätt att för sin tillsyn på begäran få

1. tillgång till de personuppgifter som behandlas,
2. upplysningar om och dokumentation av behandlingen av personuppgifter och säkerheten vid denna, och
3. tillträde till sådana lokaler som har anknytning till behandlingen av personuppgifter.

27 § Om tillsynsmyndigheten konstaterar att en myndighet kan komma att behandla personuppgifter på ett olagligt sätt, ska tillsynsmyndigheten genom påpekanden eller andra åtgärder som inte är tvingande försöka åstadkomma att myndigheten uppfyller sina skyldigheter enligt denna lag eller föreskrifter som meddelats med stöd av den.

28 § Tillsynsmyndigheten får förelägga en myndighet att uppfylla sina skyldigheter, om myndigheten inte uppfyller de krav som följer av denna lag eller föreskrifter som meddelats med stöd av den.

Av föreläggandet ska framgå vad tillsynsmyndigheten anser är nödvändigt för att avhjälpa de påtalade bristerna.

29 § Om en myndighet allvarligt brister i sin skyldighet att uppfylla de krav som gäller för en behandling av personuppgifter som myndigheten utför, får tillsynsmyndigheten förbjuda myndigheten att fortsätta behandlingen på något annat sätt än att personuppgifter lagras. Ett beslut om förbud mot fortsatt behandling gäller omedelbart.

30 § Tillsynsmyndigheten får hos förvaltningsrätten inom vars domkrets tillsynsmyndigheten är belägen ansöka om att sådana personuppgifter som har behandlats på ett olagligt sätt ska utplånas.

Bemyndiganden

31 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om

1. när behandling av personuppgifter är tillåten,
2. vilka krav som ställs på en personuppgiftsansvarig myndighet, och
3. att känsliga personuppgifter får behandlas om det behövs med hänsyn till ett viktigt allmänt intresse.

Regeringen får meddela föreskrifter om begränsningar av möjligheterna att använda andra sökbegrepp än de som avses i 12 §.

Överklaganden

32 § Tillsynsmyndighetens beslut enligt denna lag om annat än föreskrifter får överklagas till allmän förvaltningsdomstol.

Tillsynsmyndigheten får bestämma att dess beslut ska gälla även om det överklagas.

33 § Beslut om rättelse eller komplettering enligt 24 §, om avskiljande eller utplåning enligt 25 § och om information enligt 26 § personuppgiftslagen (1998:204) får överklagas till allmän förvaltningsdomstol.

Första stycket gäller inte för beslut av regeringen, Högsta domstolen, Högsta förvaltningsdomstolen eller riksdagens ombudsmän.

34 § Andra beslut enligt denna lag än sådana som avses i 32 § och 33 § första stycket får inte överklagas.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Övergångsbestämmelser

1. Denna lag träder i kraft den 1 januari 2017.
2. Bestämmelserna i 21 § ska inte börja tillämpas förrän den 1 januari 2019 i fråga om avtal som ingåtts före ikraftträdandet.
3. Bestämmelserna i 28 § personuppgiftslagen (1998:204) ska tillämpas i stället för 24 och 25 §§ i fråga om en begäran som gjorts före ikraftträdandet.

1.2 Förslag till lag om ändring i offentlighets- och sekretesslagen (2009:400)

Härigenom föreskrivs att 10 kap. 28 § offentlighets- och sekretesslagen ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*

10 kap.

28 §

Sekretess hindrar inte att en uppgift lämnas till en annan myndighet, om uppgiftsskyldighet följer av lag eller förordning.

Sekretess hindrar inte heller att en uppgift lämnas till en annan myndighet genom direktåtkomst enligt vad som föreskrivs i lag eller förordning.

Ytterligare sekretessbrytande bestämmelser och bestämmelser om undantag från sekretess finns i anslutning till berörda sekretessbestämmelser i avdelning IV–VI.

Denna lag träder i kraft den 1 januari 2017.

2 Vårt uppdrag och arbete

2.1 Uppdraget

Vi har haft som övergripande uppdrag att se över den s.k. registerlagstiftningen, som kompletterar personuppgiftslagen (1998:204) och innehåller bestämmelser om statliga och kommunala myndigheters behandling av personuppgifter. Detta ska ske genom att utreda förutsättningarna för att skapa en generell, enhetlig och – helt eller i vart fall delvis – samlad reglering för myndigheternas personuppgiftsbehandling. Om vi bedömer att det finns sådana förutsättningar ska vi lämna de författningsförslag som vi anser vara motiverade.

Det fastlagda målet för vårt arbete är att regleringen ska utgöra en tydlig och lättillämpad helhet tillsammans med tryckfrihetsförordningen och offentlighets- och sekretesslagen. På så sätt skapas rättsliga förutsättningar för en mer effektiv e-förvaltning, där såväl den enskildes rätt till personlig integritet som allmänhetens berättigade anspråk på insyn i den offentliga verksamheten tillgodoses.

De förslag som lämnas ska vidare vara anpassade till det pågående arbetet inom EU med att reformera den unionsrättsliga dataskyddsregleringen utifrån kommissionens förslag den 25 januari 2012 till Europaparlamentets och rådets förordning om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (allmän uppgiftsskyddsförordning). Personuppgiftsbehandling inom den brottsbekämpande verksamheten omfattas inte av vårt uppdrag.

I uppdraget ingår att göra en översiktlig inventering av registerförfattningarna. Vidare ingår ett antal särskilda delfrågor. En av dessa – om det finns anledning att ändra definitionen av begreppet allmän handling i tryckfrihetsförordningen i fråga om uppgifter som en myndighet har tillgång till genom s.k. direktåtkomst hos en annan myndighet eller genom liknande former av elektroniskt utlämnande –

har vi redovisat genom delbetänkandet Överskottsinformation vid direktåtkomst (SOU 2012:90). Bland återstående delfrågor finns frågan om det finns skäl att behålla den rättsliga åtskillnaden mellan olika former av elektroniskt utlämnande samt frågan om det finns anledning att justera 6 kap. 5 § OSL, som föreskriver en skyldighet att lämna uppgift till annan myndighet, så att bestämmelsen står i bättre överensstämmelse med förekomsten av användningsbegränsningar i internationella avtal m.m.

Enligt våra ursprungliga direktiv skulle vårt arbete med översynen av registerförfattningarna utmynna i utarbetandet av en generell regleringsmodell för hur registerförfattningar bör struktureras, vilka begrepp som bör användas och hur begreppen bör definieras. Med en generell modell som mall skulle vi lämna konkreta förslag till registerförfattningar – modellregleringar – inom tre olika verksamhetsområden. Avsikten var att regeringen i tilläggsdirektiv, efter att ha inhämtat synpunkter från utredaren, skulle närmare ange vilka verksamhetsområden som regleringsmodellen skulle appliceras på.

Hösten 2013 lämnade vi i en framställning till regeringen några synpunkter på inriktningen av det fortsatta arbetet. I framställningen lyfte vi fram två faktorer som vi menade borde beaktas i våra kommande tilläggsdirektiv.

Den första faktorn var att vi under vårt arbete med att inventera registerförfattningarna och identifiera vilka närmare problemområden som fanns hade uppmärksammat att den övergripande problembilden med registerförfattningarna inte bara sammanhängde med utformningen av författningarna utan också med det förhållandet att den allmänna regleringen i personuppgiftslagen i ett flertal avseenden är utformad utan hänsyn till de särskilda förhållanden som gäller för myndigheternas personuppgiftsbehandling. Vi identifierade alltså ett behov av att behandla frågor som inte är begränsade till registerförfattningsreglerade områden utan som gäller generellt inom myndighetsområdet.

Den andra faktorn var att det efter hand föreföll allt mer angeläget att anpassa det fortsatta utredningsarbetet till det parallellt pågående reformarbetet beträffande den unionsrättsliga dataskyddsregleringen innefattande det förslag till ny förordning som kommissionen hade lämnat en tid efter det att våra första direktiv beslutats.

Den 6 mars 2014 beslutades tilläggsdirektiv med bl.a. ändrad inriktning av uppdraget vad gäller metoden för översynen och inrikt-

ningen på vad arbetet ska utmynna i. Direktiven till utredningen (dir. 2011:86, 2014:31 och 2014:147) finns intagna i betänkandet som bilagorna 1–3.

2.2 Utredningsarbetet

Vårt delbetänkande

Vårt arbete inleddes med att behandla delfrågan om en eventuell ändring av begreppet allmän handling i tryckfrihetsförordningen. Den närmare frågeställningen gällde om det fanns anledning att inskränka handlingsoffentligheten såvitt avsåg överskottsinformation vid direktåtkomst. Med överskottsinformation avsågs i det sammanhanget externt tillgängliga personuppgifter som en mottagande myndighet vid direktåtkomst till en annan myndighets elektroniska informationssamling tekniskt sett har tillgång till men som den mottagande myndigheten antingen inte får ta del av i ett enskilt fall, därför att vissa rättsliga förutsättningar inte föreligger, eller får men faktiskt ännu inte har tagit del av i sin verksamhet. Frågeställningen bottnar i det förhållandet att det för frågan om vilka elektroniska upptagningar som en myndighet förvarar, och därmed vad som konstituerar en allmän handling, inte spelar någon roll om en mottagande myndighet i ett enskilt fall faktiskt har utnyttjat möjligheten att söka fram en upptagning eller inte. Redan det förhållandet att det går att göra detta räcker för att upptagningen ska bli en allmän handling hos den mottagande myndigheten. Överskottsinformation uppstår därför att det när direktåtkomst etableras inte går att på förhand avgöra exakt vilka specifika uppgifter i den utlämnande myndighetens informationssamlingar som en mottagande myndighet i konkreta fall kommer att behöva ta del av.

Vår samlade bedömning blev att en grundlagsändring med sikte enbart på överskottsinformation vid direktåtkomst inte borde föreslås. Däremot förordade vi – med anledning av ytterligare problemställningar som vi stötte på vid sidan om den grundlagsfråga som omfattades av vårt uppdrag – en allmän översyn av begreppet inkommen allmän handling i den elektroniska miljön.

Mot bakgrund av att vi inte föreslog en grundlagsändring behandlade vi i delbetänkandet frågan om sekretess för överskottsinformation hos mottagande myndigheter. Vi fann därvid att bestäm-

melsen om överföring av sekretess vid direktåtkomst enligt 11 kap. 4 § OSL i och för sig är ändamålsenligt utformad men att konstruktionen för konkurrensbestämmelsen i 11 kap. 8 § OSL – om att s.k. primär sekretess hos en mottagande myndighet ska tillämpas i stället för en överförd sekretess – medför en risk för att överskottsinformation får ett försämrat sekretesskydd hos mottagande myndigheter. Vi fann också att en sådan försämring inte är motiverad utifrån något insynsintresse. Vi föreslog därför en justering av 11 kap. 8 § OSL av innebörd att en från den utlämnande myndigheten överförd sekretessreglering ska tillämpas på överskottsinformation om den mottagande myndigheten enligt lag eller förordning inte får behandla informationen och en tillämpning av offentlighets- och sekretesslagens huvudregel om konkurrens mellan sekretessbestämmelser i 7 kap. 3 § OSL leder till att uppgifterna i fråga är sekretessbelagda enligt den överförda sekretessregleringen.

Arbetet med grundlagsfrågan om överskottsinformation vid direktåtkomst avslutades genom att vi i januari 2013 lämnade ovan nämnda delbetänkande. Under denna del av vårt arbete fanns det en parlamentarisk referensgrupp knuten till utredningen.

Arbetets bedrivande efter delbetänkandet

Utredningens fortsatta arbete har bedrivits på sedvanligt sätt med regelbundna sammanträden med expertgruppen. Första sammanträdet i det återstående uppdraget hölls den 25 januari 2013. Därefter har ytterligare tio sammanträden hållits. Även informella kontakter inom utredningen har förekommit.

Under den aktuella utredningstiden har utredaren samrått med E-delegationen (N Fi 2009:01), Uppgiftslämnarutredningen (N 2012:01) och PSI-utredningen (S 2013:02). Samråd har vidare ägt rum med de myndigheter som anges i direktiven. Vi har också sammanträffat med samtliga justitieombudsmän, Riksarkivet och Försäkringskassan.

Sekretariatet har besökt eller haft andra särskilda möten med E-hälsomyndigheten, Justitiekanslern, Lantmäteriet, Myndigheten för samhällsskydd och beredskap, Skatteverket, Sveriges Kommuner och Landsting, samt Transportstyrelsen. Sekretariatet har också träffat företrädare för näringslivet. Nämnda möten har i allt väsentligt syftat

till att inhämta information och synpunkter i frågor som rör utredningsuppdraget.

För att få ytterligare underlag i vårt översynsarbete har vi inbjudit myndigheter, enskilda företag och andra intressenter att lämna synpunkter och bidra med erfarenheter utifrån ett antal frågeställningar rörande registerförfattningar. Vi fick därvid bistånd av E-delegationen och Sveriges Kommuner och Landsting med att sprida frågorna till möjliga intressenter. Svar inkom från såväl statliga som kommunala myndigheter. Även ett antal näringsidkare besvarade frågeställningarna, såsom Bisnode och Upplysningscentralen (UC) vilka båda bedriver verksamhet med s.k. vidareutnyttjande av offentlig information.

Datainspektionen och Myndigheten för samhällsskydd och beredskap har bistått utredningen med underlag angående frågor om informationssäkerhet och skydd för personuppgifter.

Härutöver har sekretariatet haft samråd eller annan dialog med ett flertal andra utredningar, bl.a. Utredningen om rätt information i vård och omsorg (S 2011:13), Statistikutredningen 2012 (Fi 2011:05), Utredningen om personuppgiftsbehandlingen vid ISF (S 2013:13), E-hälsokommittén (S 2013:17), Integritetskommittén (Ju 2014:09) och 2014 års Utlänningsdatautredning (Ju 2014:11).

Utredare och sekretariat har deltagit i olika konferenser och seminarier med anknytning till utredningsuppdraget.

Arbetet har bedrivits med aktivt deltagande av och i samråd med experterna. Med hänsyn till detta redovisas arbetet i denna del av vårt uppdrag med användande av vi-form, även om det inte funnits fullständig samsyn i alla delar.

2.3 Slutbetänkandets disposition m.m.

Framställningen i det följande inleds med en allmän bakgrund där vi i kapitel 3 redogör kort för bl.a. it-politik, gällande rätt och kommissionens förslag till uppgiftsskyddsförordning. I kapitel 4 beskrivs översiktligt registerlagstiftningsområdet och vår inventering av detta. I kapitel 5 redovisas våra överväganden angående delfrågan om det finns skäl att behålla den rättsliga åtskillnaden mellan olika former av elektroniskt utlämnande. I kapitel 6 behandlas delfrågan om det finns anledning att justera 6 kap. 5 § OSL med anledning av före-

komsten av användningsbegränsningar i internationella avtal m.m. I återstående kapitel, kapitel 7–21, redovisas våra överväganden och förslag i fråga om en generell, enhetlig och samlad reglering för myndigheters behandling av personuppgifter.

I viss utsträckning förekommer en del upprepningar vad gäller redovisning av gällande rätt m.m. Avsikten med detta är att underlätta separat läsning av varje kapitel utan alltför omfattande hänvisningar till tidigare kapitel i betänkandet.

Det kan observeras att vi i det följande omväxlande använder termerna persondataskyddsreglering och dataskyddsreglering som benämning på det rättsområde med särskild inriktning på att reglera behandling av personuppgifter som är helt eller delvis automatiserad eller som ingår i manuella register. Någon betydelseskillnad mellan termerna är inte avsedd.

Det kan också noteras att vi i det följande använder benämningen ”brottsbekämpande verksamhet” i en tämligen vidsträckt bemärkelse. Vad som avses är sådan verksamhet som inte omfattas av kommissionens förslag till uppgiftsskyddsförordning utan av ett förslag till Europaparlamentets och rådets direktiv om skydd för enskilda personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter.

ALLMÄN BAKGRUND

3 Allmänna förutsättningar

3.1 It-politik m.m.

3.1.1 Informationssamhället och den offentliga förvaltningen

Elektronisk informationshantering infördes förhållandevis tidigt i den svenska offentliga förvaltningen. Välfärdsstatens socialförsäkringsprogram förutsatte bl.a. en automatiserad registerföring av hög standard. Myndigheterna byggde därför tidigt upp olika typer av dataregister som blev centrala i verksamheten. Utveckling av s.k. e-förvaltning blev också tidigt ett viktigt medel för att genomföra besparingar och effektiviseringar i förvaltningen. När internet introducerades på 1990-talet hade myndigheterna redan en relativt hög teknikmognad och e-tjänster blev ett sätt att underlätta kontakten utåt. Elektroniskt informationsutbyte kunde vidare ersätta andra metoder att utbyta information mellan myndigheter (se bl.a. SOU 2009:86 s. 33 f.).

Vid tiden för millennieskiftet konstaterade regeringen att samhället stod mitt uppe i en samhällsomvandling och man talade om ”den digitala revolutionen” eller ”IT-revolutionen” (prop. 1999/2000:86 s. 13). Regeringen konstaterade vidare att informationstekniken snart skulle komma att finnas representerad överallt i samhället och ”informationssamhället” blev ett begrepp. Som it-politiskt mål sattes att Sverige som första land skulle bli ett informationssamhälle för alla. Vidare fastslogs strategin för 24-timmarsmyndigheter som skulle vara elektroniskt tillgängliga dygnet runt för informationsinhämtande, ärendehantering eller annan service (a. prop. s. 24 och s. 100 f.). Syftet var att myndigheterna skulle öka tillgängligheten av tjänsteutbudet. Strategin byggde på en redan framgångsrik tradition där myndigheterna själva bestämde hur it bäst skulle användas för att utveckla verksamheten.

Flertalet myndigheter har numera webbaserade e-tjänster som vänder sig till medborgare och företag. Några exempel är Skatteverkets och Försäkringskassans e-tjänster för skattedeklarationer, begäran om sjukpenning m.m. Hos många kommuner kan invånarna via internet ha kontakt med vård och skola, ansöka om ekonomiskt bistånd eller bygglov m.m. Vid årsskiftet 2013/14 hade ca 30 procent av myndigheterna s.k. mobila appar, drygt 70 procent använde sociala medier i kontakten med enskilda och över hälften av myndigheterna använde sig av s.k. molntjänster i någon form (Skr. 2013/14:155 s. 27). Digitala ärendehanteringssystem där all information i ett ärende samlas i en elektronisk akt blir allt vanligare. Ett digitalt ärendehanteringssystem består normalt av ett elektroniskt diarium, ett elektroniskt system för handläggning i elektroniska akter där även skannade inlagor på papper lagras och ett digitalt arkiv. I dag används it både för att hantera information om verksamheten och som en del i verksamheten som sådan. Inom exempelvis den offentliga hälso- och sjukvården sker såväl vårddokumentation, patientjournalföring m.m. som faktiskt utförande av vård, t.ex. vid ultraljudsundersökningar och operationer, med användning av it.

3.1.2 Aktuell it-politik och strategi

Ett nytt mål för it-politiken beslutades av riksdagen 2011 (prop. 2011/2012:1, 2011/12:TU1). Målet är att Sverige ska vara bäst i världen på att använda digitaliseringens möjligheter. För att uppnå detta krävs ökad digital delaktighet så att fler vill och vågar använda digitala tjänster. Det krävs även fler tjänster som gör att människor upplever att de verkligen har nytta av att använda internet. Ett delmål är att Sverige ska ha bredband i världsklass. Alla hushåll och företag bör ha goda möjligheter att använda sig av elektroniska samhällstjänster och service via bredband (prop. 2009/10:193). Målet gäller fortfarande (2014/15:TU1 s. 15 f., jfr prop. 2014/15:1 utgiftsområde 22 s. 126).

I september 2011 beslutade regeringen om en ny strategi för it-politiken, It i människans tjänst – en digital agenda för Sverige (dnr N2011/342/ITP). Agendan är en sammanhållen strategi för it-politiken som syftar till att statens befintliga resurser ska utnyttjas

bättre. I den digitala agendan har regeringen presenterat ambitioner och insatser som tillvaratar de möjligheter som digitaliseringen ger. För att nå det ovannämnda it-politiska målet har med utgångspunkt i it-användarens perspektiv fyra strategiska områden identifierats i agendan: 1. lätt och säkert att använda, 2. tjänster som skapar nytta, 3. det behövs infrastruktur och 4. it:s roll för samhällsutvecklingen.

I juni 2012 tillsatte regeringen Digitaliseringskommissionen som har i uppdrag att verka för att det it-politiska målet i agendan uppnås och att regeringens ambitioner inom området fullföljs (dir. 2012:61). En del av kommissionens uppdrag är att ta fram indikatorer för att mäta måluppfyllelsen. Slutredovisning av uppdraget ska ske senast den 31 december 2015.

3.1.3 Förvaltningspolitik och e-förvaltning

Hur den offentliga förvaltningen utvecklas, organiseras och styrs har stor betydelse för myndigheternas informationshantering. I 2010 års förvaltningspolitiska proposition lade regeringen fram mål och riktlinjer för det fortsatta arbetet med i första hand den statliga förvaltningen. Det övergripande målet för förvaltningspolitiken ska vara en innovativ och samverkande statsförvaltning som är rättssäker och effektiv, har en väl utvecklad kvalitet, service och tillgänglighet och därigenom bidrar till Sveriges utveckling och ett effektivt EU-arbete. Målet har antagits av riksdagen och är alltjämt gällande (prop. 2009/10:175 samt prop. 2014/15:1 utgiftsområde 2). Samverkan, inte minst myndigheter emellan, ska ytterligare utvecklas, dels av effektivitetsskäl, dels för att medborgare, företagare och andra förväntar sig att staten uppträder samordnat. Förstärkt samverkan mellan statsförvaltningen och kommunerna inom vissa områden finns också på den förvaltningspolitiska dagordningen. Elektronisk förvaltning (e-förvaltning) ska bidra till det förvaltningspolitiska målet.

E-förvaltning är ett begrepp som används för att beskriva en form av verksamhetsutveckling inom den offentliga förvaltningen som innebär att myndigheterna drar nytta av it och kombinerar den nya tekniken med organisatoriska förändringar och satsningar på kompetensutveckling i syfte att förbättra effektiviteten i sina respek-

tive verksamheter. Benämningen e-förvaltning används också för att beskriva statsförvaltningens användning av it för utbyte av information och tjänster med medborgare, företag och andra delar av förvaltningen. E-förvaltning är också en viktig del i den digitala agendans strategiska område 2. ”tjänster som skapar nytta”.

I januari 2008 fastställde regeringen en nationell handlingsplan för den svenska e-förvaltningen (Fi2008/491). I denna anges det övergripande målet för e-förvaltningen vara att arbetet ska leda till att det ska vara så enkelt som möjligt för så många som möjligt att utöva sina rättigheter och fullgöra sina skyldigheter samt ta del av förvaltningens service. Service till medborgare och företag står i fokus. Det övergripande målet ska uppnås med hjälp av insatser inom följande fyra områden; regelverk för myndighetsövergripande samverkan och informationshantering, tekniska förutsättningar och it-standardisering, gemensamma verksamhetsstöd, kompetensförsörjning och samlad uppföljning samt förvaltningens kontakter med medborgare och företag. Det gemensamma arbetet är inriktat mot tre målbilder; en enklare vardag för företag och privatpersoner, en öppnare och smartare förvaltning som stödjer innovation och delaktighet samt en effektivare offentlig verksamhet (prop. 2011/12:1 utgiftsområde 22 s. 85). I mars 2009 tillsattes E-delegationen som ett led i genomförandet av handlingsplanen för e-förvaltning.

Den 17 december 2012 presenterade regeringen en ny strategi: Med medborgaren i centrum – Regeringens strategi för en digitalt samverkande statsförvaltning (N2012/6402/ITP). I strategin beskrivs regeringens målsättningar för arbetet med att styra och förstärka myndigheternas förmåga att samverka digitalt i förvaltningsgemensamma it-frågor. Den enskilda medborgarens och företagarens behov ska därvid vara i centrum för utvecklingen av framtidens digitala samhällsservice. Fler förvaltningsgemensamma digitala tjänster ska bidra till att förenkla vardagen för privatpersoner och företag. De ska utformas efter användarnas behov, vara enkla och säkra att använda och lätta för medborgare att hitta. Genom att göra det lättare att hitta och använda sådan statlig information som kan vidareutnyttjas och sådana statliga tjänster som har gränssnitt som kan användas av andra system ska innovation stödjas. Publicering av offentlig information via internet och användning av sociala medier ska öka möjligheterna till insyn och delaktighet. Kvaliteten och effektiviteten i statsförvaltningen ska öka genom standardiserad

informationshantering, förbättrad informationssäkerhet och digitaliserade processer. En viktig utgångspunkt i all utveckling av statsförvaltningens tjänster är att effektivitet och service alltid måste vägas mot skyddet för den enskildes integritet och behov av sekretesskydd. Målen ska ligga till grund för regeringens koordinering och prioritering av förvaltningsgemensamma utvecklingsprojekt.

I budgetpropositionen för 2015 annonserade regeringen en förstärkt styrning och samordning av den övergripande it-användningen i statsförvaltningen genom en fyraårig satsning under åren 2015–2018. Syftet är att nå målen för e-förvaltningen samt främja utvecklingen och användningen av gemensamma lösningar. Satsningen omfattar ett flertal insatser, bl.a. avser regeringen öka styrningen av myndigheters anslutning till gemensamma e-tjänster och peka ut förvaltningsansvar för gemensamma lösningar och förmågor som krävs för en digitalt samverkande förvaltning. Vidare ska uppföljningen av myndigheternas it-användning förstärkas. I december 2014 beslutade riksdagen tillföra ytterligare medel till satsningen (2014/15:TU1 s. 51 anslaget 2:6 Gemensamma e-förvaltningsprojekt av strategisk betydelse, jfr prop. 2014/15:1 utgiftsområde 2 s. 68 och utgiftsområde 22 s. 148 f.).

I vårt delbetänkande Överskottsinformation vid direktåtkomst (SOU 2012:90) har vi i korthet beskrivit några exempel på aktuella aktörer och initiativ eller utvecklingsprojekt inom e-förvaltningen som pågått parallellt med vårt arbete, vi hänvisar till den beskrivningen (a. bet. s. 29 f.).

3.1.4 E-förvaltning inom EU

Inom EU bedrivs ett aktivt arbete med att främja utvecklingen av informationssamhället inom Europa. Den 29 april 2010 lade Europeiska kommissionen fram en digital agenda för Europa som är ett av sju ”flaggskeppsinitiativ” i EU:s övergripande strategi för tillväxt EU2020 (KOM[2010] 245 slutlig respektive KOM[2010] 2020 slutlig). Det huvudsakliga målet med agendan är att utveckla en digital inre marknad för att styra Europa mot en smart och hållbar tillväxt för alla. Utvecklandet av en modern e-förvaltning är en viktig del i den digitala agendan.

Den 15 december 2010 lade kommissionen fram en handlingsplan 2011–2015 för e-förvaltning (KOM[2010] 743 slutlig). Syftet med planen är att främja framväxten av en ny generation av öppna, flexibla och samverkande e-förvaltningstjänster för medborgare och företag. Dessa tjänster ska kunna öka medborgarnas och företagarnas egenmakt, öka rörligheten på den inre marknaden och sörja för att den offentliga sektorn stödjer en ekonomi baserad på framtida nätverk. Handlingsplanen identifierar fyra politiska prioriteringar. Medlemsstater ska använda e-förvaltning för följande ändamål: 1. öka medborgares och företags egenmakt, 2. öka rörligheten på den inre marknaden, 3. öka effektiviteten i offentlig sektor och 4. skapa nödvändiga möjliggörare och förutsättningar för att detta ska kunna ske.

Utöver den digitala agendan och handlingsplanen finns ett antal EU-direktiv och andra rättsakter, ytterligare handlingsplaner eller rekommendationer och pågående projekt och andra samarbeten mellan EU:s medlemsstater.

3.2 Rättslig reglering till skydd för personuppgifter

3.2.1 Internationella åtaganden avseende dataskydd

Förenta Nationernas allmänna förklaring om de mänskliga rättigheterna m.m.

Förenta nationernas (FN) generalförsamling antog år 1948 en universell deklaration om de mänskliga rättigheterna – Förenta Nationernas allmänna förklaring om de mänskliga rättigheterna. Deklarationen är inte formellt bindande för medlemsstaterna, men har betydelse som ett uttryck för vad den internationella opinionen kräver. I artikel 12 sägs att ingen ”må utsättas för godtyckliga ingripanden i fråga om privatliv, familj, hem eller korrespondens, ej heller angrepp på heder och anseende” samt att envar har rätt till lagens skydd mot sådana ingripanden eller angrepp. Vidare sägs i artikel 29 att endast sådana inskränkningar i de i deklarationen angivna fri- och rättigheterna är tillåtna som fastställts i lag i uteslutande syfte att trygga tillbörlig hänsyn till och respekt för andras fri- och rättigheter samt för att tillgodose det demokratiska samhällets rättmätiga krav på moral, allmän ordning och allmän välfärd.

Inom FN har också utarbetats en internationell konvention om medborgerliga och politiska rättigheter, som antogs av generalförsamlingen år 1966. Sverige anslöt sig till konventionen år 1971, varefter konventionen trädde i kraft år 1976. I konventionen behandlas vad som hör till skyddet för den personliga integriteten främst i artikel 17. Enligt denna artikels punkt 1 bör ingen utsättas för godtyckliga eller olagliga ingripanden i sitt privat- och familjeliv, sitt hem eller sin korrespondens, ej heller för olagliga angrepp på sin heder och sitt anseende. Vidare sägs i punkt 2 att envar har rätt till lagens skydd mot sådana ingripanden eller angrepp. De stater som har tillträtt konventionen åläggs således vissa skyldigheter. Ett särskilt inrättat organ benämnt Kommittén för de mänskliga rättigheterna (Human Rights Committee) övervakar att de till konventionen anslutna staterna efterlever sina skyldigheter. Förenta nationernas generalförsamling antog även år 1990 riktlinjer om datoriserade register med personuppgifter.

Europakonventionen

Den europeiska konventionen av den 4 november 1950 om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) är sedan den 1 januari 1995 inkorporerad i svensk rätt och gäller här i landet som lag (prop. 1993/94:117, 1993/94:KU24). Den har alltså inte getts ställning som grundlag. I 2 kap. 19 § RF har emellertid införts en bestämmelse om att lag eller annan föreskrift inte får meddelas i strid med Sveriges åtaganden på grund av konventionen.

Av betydelse för skyddet för den personliga integriteten är framför allt artikel 8 i konventionen. Där stadgas att var och en har rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. En offentlig myndighet får inte inskränka åtnjutande av denna rättighet annat än med stöd av lag och om det i ett demokratiskt samhälle är nödvändigt med hänsyn till statens säkerhet, den allmänna säkerheten, landets ekonomiska välstånd eller till förebyggande av oordning eller brott eller till skydd för hälsa eller moral eller för andra personers fri- och rättigheter.

Det står klart att behandling av personuppgifter och t.ex. rätt till tillgång till registrerade personuppgifter i och för sig kan falla inom

tillämpningsområdet för artikel 8 i Europakonventionen. All slags behandling av personuppgifter omfattas dock inte, utan frågan måste gälla privatliv, familjeliv, hem eller korrespondens. Primärt innebär artikel 8 att staten ska avhålla sig från ingrepp i den skyddade rättigheten. Artikeln innebär även en skyldighet för staten att vidta positiva åtgärder för att skydda den enskildes privatsfär. Sådana positiva åtgärder kan utgöras av lagstiftning, men också ha till ändamål att på annat sätt tillförsäkra medborgarna skydd mot övergrepp i särskilda situationer (Hans Danelius, Mänskliga rättigheter i europeisk praxis, 4 uppl. 2012, s. 347). I sin praxis har Europadomstolen också framhållit att kravet på att ingreppet ska vara nödvändigt inte är synonymt med ”oundgängligt”. Vad som krävs är däremot att det finns ett ”angeläget samhälleligt behov”. Inskränkningen i den grundläggande rättigheten måste vidare stå i rimlig proportion till det syfte som ska tillgodoses genom inskränkningen. Varje konventionsstat har själv en viss frihet att avgöra om en inskränkning är nödvändig. Europadomstolen förbehåller sig dock rätten att övervaka om denna frihet utnyttjas på ett rimligt sätt.

EU-domstolen har slagit fast att bestämmelserna i artikel 8 i Europakonventionen har betydelse vid sidan av det s.k. dataskyddsdirektivet vid bedömningen av nationella regler som tillåter behandling av personuppgifter (dom den 20 maj 2003 i mål C-465/00, C-138 och 139/01, Österreichiscer Rundfunk m.fl.)

Europarådets dataskyddskonvention

Europarådets ministerkommitté antog år 1981 en konvention (nr 108) till skydd för enskilda vid automatisk databehandling av personuppgifter, den s.k. dataskyddskonventionen (se prop. 1981/82:189). Konventionen trädde i kraft den 1 oktober 1985. Konventionens syfte är att säkerställa respekten för grundläggande fri- och rättigheter, särskilt den enskildes rätt till personlig integritet i samband med automatisk databehandling av personuppgifter. Utgångspunkten är att vissa av den enskildes rättigheter kan behöva skyddas i förhållande till den princip om fritt flöde av information, oberoende av gränser, som finns inskriven i internationella överenskommelser om mänskliga rättigheter. Konventionens tillämpningsområde är enligt huvudregeln automatiserade personregister och automatisk

databehandling av personuppgifter i allmän och enskild verksamhet. I konventionen anges krav på beskaffenheten av de personuppgifter som undergår automatisk databehandling, bl.a. krav på att uppgifterna ska inhämtas och behandlas på ett korrekt sätt och vara relevanta med hänsyn till ändamålet, att vissa typer av uppgifter inte får undergå automatisk databehandling om inte den nationella lagen ger ett ändamålsenligt skydd, samt att lämpliga säkerhetsåtgärder ska vidtas för att skydda personuppgifter gentemot oavsiktlig eller otillåten förstörelse. Inom Europarådet pågår en översyn av konventionen.

Inom Europarådet har vidare utarbetats ett flertal rekommendationer på dataskyddsområdet.

Riktlinjer från OECD

Inom Organisationen för ekonomiskt samarbete och utveckling, OECD, har en expertgrupp utarbetat vissa riktlinjer i fråga om integritetsskyddet och persondataflödet över gränserna. Riktlinjerna antogs år 1980 av OECD:s råd tillsammans med en rekommendation till medlemsländernas regeringar om att beakta riktlinjerna i nationell lagstiftning. Samtliga medlemsländer, däribland Sverige, har godtagit rekommendationen och åtagit sig att följa denna. Riktlinjerna är tillämpliga på personuppgifter inom både den offentliga och privata sektorn. De gäller både för uppgifter som lagras automatiskt och som förs manuellt. Syftet är emellertid att undvika de risker för personlig integritet och individens frihet som personuppgifter kan utgöra på grund av det sätt på vilket de behandlas, på grund av uppgifternas natur eller på grund av de sammanhang i vilka de används. År 2013 reviderades riktlinjerna genom införandet av vissa nyheter och förändringar.

EU:s stadga om de grundläggande rättigheterna

Lissabonfördraget innebär att Europeiska unionens stadga om de grundläggande rättigheterna, tillkännagiven av parlamentet, rådet och kommissionen den 7 december 2000 och anpassad den 12 december 2007, numera är rättsligt bindande. En referens till stadgan har införts i artikel 6.1 i unionsfördraget. I stadgan bekräftas de rättig-

heter som har sin grund i medlemsstaternas gemensamma författningstraditioner och internationella förpliktelser, Europakonventionen, unionens och Europarådets sociala stadgor samt rättspraxis från Europeiska unionens domstol och Europeiska domstolen för de mänskliga rättigheterna. Stadgans syfte är att kodifiera de grundläggande fri- och rättigheter som EU redan erkänner.

I stadgans artikel 7 föreskrivs att var och en har rätt till respekt för sitt privatliv och familjeliv, sin bostad och sin korrespondens. I artikel 8 föreskrivs vidare att var och en har rätt till skydd av de personuppgifter som rör honom eller henne. Dessa uppgifter ska behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund. Var och en har rätt att få tillgång till insamlade uppgifter som rör honom eller henne och att få rättelse av dem.

Stadgan riktar sig till verksamhet som utförs av EU:s egna organ och institutioner och den blir tillämplig för medlemsstaterna endast i de fall där de tillämpar EU-rätten (artikel 51).

När det gäller de garanterade rättigheternas räckvidd följer av artikel 52 i stadgan att varje begränsning i utövningen av de rättigheter och friheter som erkänns i stadgan ska vara föreskriven i lag och vara förenlig med proportionalitetsprincipen och det väsentliga innehållet i fri- och rättigheterna. I den mån rättigheterna i stadgan motsvarar rättigheter som skyddas av Europakonventionen ska de ha samma innebörd och räckvidd som enligt konventionen. Stadgans artiklar får inte tolkas som att de inskränker eller inkräktar på rättigheter enligt andra konventioner eller överenskommelser om fri- och rättigheter.

Dataskyddsdirektivet m.m.

Den 24 oktober 1995 antogs Europaparlamentets och rådets direktiv 95/46/EG om skydd för enskilda personer med avseende på behandling personuppgifter och om det fria flödet av sådana uppgifter (dataskyddsdirektivet). Direktivet syftar till att garantera en hög och i alla medlemsstater likvärdig skyddsnivå när det gäller enskilda personers fri- och rättigheter med avseende på behandling av personuppgifter och att främja ett fritt flöde av personuppgifter mellan medlemsstaterna i EU. Medlemsstaterna får inom den ram

som anges i direktivet närmare precisera villkoren för när behandling av personuppgifter får förekomma. Sådana preciseringar får dock inte hindra det fria flödet av personuppgifter inom unionen. Direktivet gäller inte för behandling av personuppgifter på områden som faller utanför unionsrätten, t.ex. allmän säkerhet, försvar, statens säkerhet och statens verksamhet på straffrättens område.

Dataskyddsdirektivet är endast tillämpligt på behandling av uppgifter om fysiska personer och berör alltså inte skyddet för juridiska personer. Direktivet omfattar inte bara automatiserad behandling, utan också manuell behandling av personuppgifter som ingår eller kommer att ingå i ett register. Direktivet omfattar inte behandling av personuppgifter för privat bruk.

Enligt dataskyddsdirektivet måste all behandling av personuppgifter vara laglig och korrekt. Uppgifterna måste vara riktiga och aktuella samt adekvata, relevanta och nödvändiga med hänsyn till de ändamål för vilka de behandlas. Ändamålen ska vara uttryckligt angivna vid tiden för insamling av uppgifterna. De ändamål för vilka uppgifterna senare behandlas får inte vara oförenliga med de ursprungliga ändamålen.

Personuppgifter får enligt direktivet behandlas bara i vissa fall. Personuppgifter får bl.a. behandlas om den registrerade otvetydigt har lämnat sitt samtycke, om behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åligger den registeransvarige eller är nödvändig för att utföra en arbetsuppgift av allmänt intresse eller som är ett led i myndighetsutövning. Personuppgifter får även behandlas om intresset av att den registeransvarige får behandla uppgifterna väger tyngre än den registrerades intresse av att de inte behandlas.

Vissa särskilda i direktivet angivna kategorier av uppgifter får som huvudregel inte behandlas. Det gäller uppgifter som avslöjar den enskildes ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse eller medlemskap i fackförening samt uppgifter som rör hälsa och sexualliv. I direktivet görs dock undantag från denna regel i vissa särskilt angivna situationer, bl.a. om det finns uttryckligt samtycke från den registrerade.

Dataskyddsdirektivet föreskriver att den registeransvarige ska informera den registrerade om att personuppgifter är föremål för behandling och därvid redogöra för ändamålet med behandlingen. Har uppgifterna inte samlats in från den registrerade själv behöver

den registeransvarige dock inte lämna någon information, om den registrerade redan känner till informationen eller om det skulle visa sig vara omöjligt eller innebära en ansträngning som inte står i proportion till nyttan. Den registrerade har dock rätt att på begäran få information om de registrerade uppgifterna. Vidare har den registrerade rätt att få sådana uppgifter som inte har behandlats i enlighet med direktivet rättade, utplånade eller blockerade. Direktivet innehåller även regler om säkerhet vid behandlingen.

På EU-nivå finns även kompletterande rättsakter till dataskyddsdirektivet, bl.a. det s.k. dataskyddsrambeslutet med särskilda regler om skydd för personuppgifter i frågor som rör polisiärt och straffrättsligt samarbete (rådets rambeslut 2008/977/RIF av den 27 november 2008 om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete).

För närvarande pågår inom EU en övergripande översyn av bl.a. dataskyddsdirektivet, se avsnitt 3.3.

3.2.2 Nationell reglering

Regeringsformen

Grundläggande bestämmelser om skydd för den personliga integriteten finns i regeringsformen. I målsättningsstadgandet i 1 kap. 2 § första stycket slås det fast att den offentliga makten ska utövas med respekt bl.a. för den enskilda människans frihet och i fjärde stycket anges bl.a. att det allmänna ska värna den enskildes privatliv och familjeliv. I 2 kap. 4 och 5 §§ finns bestämmelser om absolut skydd mot allvarliga fysiska integritetsintrång bl.a. döds- och kroppsstraff. Enligt 6 § samma kapitel är var och en därutöver skyddad gentemot det allmänna mot bl.a. påtvingande kroppsliga ingrepp.

Den 1 januari 2011 trädde en ny bestämmelse, 2 kap. 6 § andra stycket RF, i kraft. Enligt bestämmelsen är var och en gentemot det allmänna skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Bestämmelsen innebär alltså att enskilda är skyddade mot åtgärder från det allmännas sida men träffar inte åtgärder som en enskild vidtar i förhållande till en annan enskild. Bakgrunden till bestämmelsen är att det ansågs finnas vissa brister i lagstiftning som innefattade intrång

i den enskildes personliga integritet. Dessa brister bestod i att de avvägningar mellan olika motstående intressen som normalt ska göras i lagstiftningsärenden i vissa fall var bristfälligt redovisade och att det i första hand var de negativa effekterna av olika integritetsbegränsande åtgärder som var knapphändigt belysta (prop. 2009/10:80 s. 175 f.). Av bl.a. dessa skäl ansågs det därför finnas ett behov av att stärka skyddet av den personliga integriteten i grundlag. Det stärkta grundlagsskyddet består i att en begränsning av det skydd som bestämmelsen föreskriver endast får göras i form av lag och under de förutsättningar som anges 2 kap. 21–22 §§ RF.

Personuppgiftslagen

Dataskyddsdirektivet har genomförts i svensk rätt genom personuppgiftslagen (1998:204). Bestämmelserna i personuppgiftslagen har till syfte att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter. Liksom den tidigare datalagen (1973:289), vilken upphävdes i och med personuppgiftslagens införande, är personuppgiftslagen generellt tillämplig och gäller både för myndigheter och enskilda som behandlar personuppgifter. Rent privat behandling av personuppgifter är dock undantagen.

Personuppgiftslagen är subsidiär i förhållande till annan lag eller förordning (2 §). Vid lagens införande anfördes att det traditionella svenska systemet med särregler i särskilda författningar var att föredra framför generella undantag från den nya lagen (prop. 1997/98:44 s. 41).

Personuppgiftslagen, som i huvudsak följer dataskyddsdirektivets text och disposition, omfattar all helt eller delvis automatiserad behandling av personuppgifter (5 § första stycket). Lagen är teknikoberoende i den meningen att den i fråga om automatiserad behandling inte begränsas till dataregister. All automatiserad behandling omfattas, alltså även personuppgifter som framgår av bilder och ljud. Begreppet register saknar betydelse för lagens tillämpning. Det avgörande är att personuppgifterna är föremål för automatiserad behandling, inte om de är ordnade i ett register eller inte. Det är vidare tillräckligt att behandlingen av personuppgifter delvis är automatiserad för att den ska falla under lagens bestämmelser.

Om uppgifter samlas in manuellt och sedan behandlas automatiserat är även insamlandet en sorts behandling som omfattas av lagen. På samma sätt faller t.ex. ett utlämnande genom manuella utskrifter från ett automatiserat register in under lagens bestämmelser. Personuppgiftslagen gäller även för manuella register med personuppgifter som är strukturerade eller ordnade så att de är sökbara på person (5 § andra stycket).

Med personuppgifter avses all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet (3 §). Begreppet behandling av personuppgift är ett vitt begrepp och omfattar varje åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter, vare sig det sker på automatisk väg eller inte. Exempel på behandling av personuppgifter är insamling, registrering, organisering, lagring, bearbetning eller ändring, återvinning, inhämtande, användning, utlämnande genom översändande, spridning eller annat tillhandahållande av uppgifter, sammanställning eller samkörning, blockering, utplåning eller förstöring (3 §).

Det finns några viktiga undantag från personuppgiftslagens tillämpningsområde. Lagen gäller t.ex. inte vid behandling av personuppgifter som en fysisk person utför som ett led i en verksamhet av rent privat natur (6 §). Bestämmelserna i lagen tillämpas inte heller i den utsträckning det skulle strida mot grundlagsbestämmelserna om tryck- och yttrandefrihet (7 § första stycket). I princip ska inte heller personuppgiftslagens bestämmelser tillämpas vid journalistisk, konstnärlig eller litterär verksamhet (7 § andra stycket). Vidare anges i personuppgiftslagen att lagen inte gäller i den mån det skulle inskränka offentlighetsprincipen (8 § första stycket).

Behandling av personuppgifter som inte ingår i eller är avsedda att ingå i en samling av personuppgifter som har strukturerats för att påtagligt underlätta sökningen efter eller sammanställningen av personuppgifter omfattas inte av flertalet av de hanteringsregler som anges i personuppgiftslagen. Det som i stället avgör om en sådan behandling är tillåten eller inte är om behandlingen innebär en kränkning av den registrerades personliga integritet (5 a §).

I 9 § ges vissa grundläggande krav på all behandling av personuppgifter som omfattas av lagen. Den personuppgiftsansvarige, vilken oftast är det organ där personuppgifterna behandlas, ska se till att personuppgifter behandlas bara om det är lagligt samt att personuppgifter alltid behandlas på ett korrekt sätt och i enlighet

med god sed. Vidare ska personuppgifter samlas in bara för särskilda, uttryckligt angivna och berättigade ändamål. Ändamålet med en behandling av personuppgifter måste bestämmas redan när uppgifterna samlas in. Den personuppgiftsansvarige ska definiera avsikten med insamlingen och användningen av personuppgifterna på ett så precist sätt som möjligt. Personuppgifterna får inte sedan behandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in (finalitetsprincipen). Det sistnämnda kan bli aktuellt att pröva när personuppgifter lämnas ut till tredje man. Ett sådant utlämnande får alltså inte vara oförenligt med det ändamål för vilket uppgifterna ursprungligen samlades in. Om personuppgifter lämnas ut i form av allmänna handlingar med stöd av bestämmelserna i 2 kap. TF blir en sådan prövning dock inte aktuell.

De personuppgifter som behandlas ska vara adekvata och relevanta i förhållande till ändamålen med behandlingen. Med detta krav avses att personuppgifterna ska vara av sådant slag att de hör till saken (relevanta) och är ägnade att uppnå det mål man har med behandlingen (adekvata). Inte heller får fler personuppgifter behandlas än vad som är nödvändigt med hänsyn till ändamålen med behandlingen. Därutöver ska de uppgifter som behandlas vara riktiga och, om det är nödvändigt, aktuella. Alla rimliga åtgärder ska vidtas för att rätta, blockera eller utplåna sådana personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålen med behandlingen. Personuppgifter får inte heller bevaras under längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen.

Varje behandling av personuppgifter måste kunna hänföras till någon av de situationer som anges i personuppgiftslagens regler om när behandling av personuppgifter är tillåten. Av 10 § följer att personuppgifter får behandlas bara om den registrerade har lämnat sitt samtycke till behandlingen, behandlingen är nödvändig för att ett avtal med den registrerade ska kunna fullgöras eller åtgärder som den registrerade begärt ska kunna vidtas innan ett avtal träffas, den personuppgiftsansvarige ska kunna fullgöra en rättslig skyldighet, vitala intressen för den registrerade ska kunna skyddas, en arbetsuppgift av allmänt intresse ska kunna utföras, den personuppgiftsansvarige eller en tredje man till vilken personuppgifter lämnas ut ska kunna utföra en arbetsuppgift i samband med myndighetsutövning, eller ett ändamål som rör ett berättigat intresse

hos den personuppgiftsansvarige eller hos en sådan tredje man till vilken personuppgifterna lämnas ut ska kunna tillgodoses, om detta intresse väger tyngre än den registrerades intresse av skydd mot kränkning av den personliga integriteten.

Enligt 11 § får inte personuppgifter behandlas för ändamål som rör direkt marknadsföring, om den registrerade hos den personuppgiftsansvarige skriftligen har anmält att han eller hon motsätter sig sådan behandling. Inte heller får personuppgifter behandlas i de fall där behandling bara är tillåten när den registrerade har lämnat sitt samtycke och han eller hon har återkallat detta (12 §). Utöver vad som följer av 11 och 12 §§ har den enskilde ingen rätt att motsätta sig sådan behandling av personuppgifter som är tillåten enligt lagen.

Enligt 13 § är det generellt sett förbjudet att behandla känsliga personuppgifter. Med känsliga personuppgifter avses sådana personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i en fackförening eller som rör hälsa eller sexualliv. Från förbudet att behandla känsliga personuppgifter finns, utöver när den registrerade har lämnat sitt samtycke (15 §), vissa undantag (16–20 §§).

Särskilda bestämmelser om uppgifter om lagöverträdelser och behandling av personnummer finns i 21 och 22 §§.

Bestämmelser om i vilka fall information om behandling av personuppgifter ska lämnas till den enskilde finns i 23–27 §§, rätt att begära rättelse och omprövning av automatiserade beslut finns i 28 och 29 §§ och föreskrifter om säkerheten vid behandling av personuppgifter finns i 30–32 §§.

Enligt 33 § är det förbjudet att till tredjeland, dvs. ett land utanför EU eller ESS, föra över personuppgifter som är under behandling, om landet inte har en adekvat nivå för skydd av personuppgifter. Förbudet gäller i princip alla slag av personuppgifter och är alltså inte begränsat till exempelvis kategorierna känsliga personuppgifter eller uppgifter om lagöverträdelser. Trots förbudet är det enligt 34 § tillåtet att under vissa förutsättningar föra över uppgifter till tredjeland men det förutsätter antingen att den registrerade gett sitt samtycke till överföringen eller att överföringen är nödvändig bl.a. för att rättsliga anspråk ska kunna fastställas, göras gällande eller försvaras eller att vitala intressen för den registrerade ska kunna skyddas. Vidare är det tillåtet att föra över personuppgifter för

användning enbart i en stat som har anslutit sig till Europarådets dataskyddskonvention. Regeringen får meddela föreskrifter om ytterligare undantag från förbudet mot överföring (35 §).

Vidare finns det i lagen bl.a. bestämmelser om anmälan till tillsynsmyndigheten, tillsyn, skadestånd och straff.

Sekretess

I offentlighets- och sekretesslagen (2009:400) finns ett stort antal bestämmelser om sekretess till skydd för uppgift om enskilds personliga förhållanden, vilka syftar till att skydda enskilds personliga integritet. Av dessa bör i detta sammanhang särskilt nämnas 21 kap. 7 § OSL, den s.k. PuL-sekretessen. Enligt bestämmelsen gäller sekretess för personuppgift, om det kan antas att ett utlämnande skulle medföra att uppgiften behandlas i strid med personuppgiftslagen. Bestämmelsen tar inte sikte på uppgifterna som sådana utan på vad mottagaren tänker göra med dem. Bestämmelsen avser alltså att ge ett skydd mot otillåten behandling av personuppgifter. Bestämmelsen är tillämplig hos alla myndigheter och vid alla utlämnanden som innefattar personuppgifter men den risk för skada som anges i bestämmelsen aktualiseras främst vid utlämnanden av en större mängd uppgifter i form av massuttag av allmänna handlingar. Också ett utlämnande av selekterade uppgifter, t.ex. uppgifter om personer med viss inkomst eller med viss politisk tillhörighet, kan indikera risk för den skada som anges i bestämmelsen.

Registerförfattningar

De s.k. registerförfattningarna har till huvudsakligt syfte att reglera inrättandet och användningen av viktigare register eller andra personuppgiftssamlingar inom den offentliga sektorn.

Registerförfattningarna reglerar myndigheternas behandling av personuppgifter och är tänkta att ge ett anpassat integritetsskydd vid myndighetens hantering av personuppgifter då behov finns att avvika från eller komplettera det integritetsskydd som personuppgiftslagen annars ger.

En utgångspunkt vid utarbetandet av registerförfattningar har varit att regleringen så långt som möjligt ska vara i överensstäm-

melse med personuppgiftslagen och därmed med dataskyddsdirektivets materiella bestämmelser samt att behovet av särregler i förhållande till personuppgiftslagen bör övervägas noga (prop. 1997/98:44 s. 41 och Sören Öman, Särskilda registerförfattningar, Festskrift till Peter Seipel, s. 694 f.).

En omständighet som ansetts tala för en särreglering i förhållande till personuppgiftslagen är att en särskild författning under vissa förutsättningar anses innebära en bättre garanti för utformningen av integritetsskyddet vad gäller särskilt känsliga register eller andra personuppgiftssamlingar.

Exempel på fall då en särskild författningsreglering i form av en registerförfattning har ansetts motiverad är vidare när en nödvändig behandling av personuppgifter över huvud taget inte är tillåten enligt personuppgiftslagen, när personuppgiftslagen visserligen reglerar ett visst förhållande men det finns anledning att avvika från eller precisera den regleringen, när personuppgiftslagens bestämmelser kan ge upphov till tolkningsproblem och det finns anledning att ha tydliga bestämmelser, när det finns anledning att begränsa möjligheterna till behandling av uppgifter av integritetsskäl i fråga om myndigheters registrering och åtkomst till stora och känsliga uppgiftsmängder eller när det finns anledning att vara särskilt tydlig gentemot allmänheten, t.ex. i fråga om vilka uppgifter om enskilda som en myndighet registrerar.

Registerförfattningar har ofta getts lagform trots att detta rent normgivningstekniskt inte har varit nödvändigt. Den bakomliggande tanken har emellertid varit att myndighetsregister med ett stort antal registrerade och med ett känsligt innehåll ska regleras särskilt genom lag (prop. 1990/91:60 s. 50, KU 1990/91:11 s. 11, se även prop. 1997/98:44 s. 41).

3.3 Pågående reformarbete inom EU

3.3.1 Allmänt

Den 25 januari 2012 presenterade kommissionen ett förslag till en genomgripande reform av EU:s regler om skydd för personuppgifter. Förslaget omfattar dels en förordning med en generell reglering som ska ersätta dataskyddsdirektivet, kallad allmän uppgiftsskyddsförordning, dels ett nytt direktiv med särregler för den brotts-

bekämpande sektorn som ska ersätta det gällande dataskyddsrambeslutet (rambeslut 2008/977/RIF). Det föreslagna direktivet är mera vidsträckt till sitt tillämpningsområde än dataskyddsrambeslutet i det att direktivet inte bara omfattar utbyte av information över gränserna utan även nationell personuppgiftsbehandling inom den brottsbekämpande sektorn.

Det huvudsakliga syftet med kommissionens förslag till uppgiftsskyddsförordning är att ytterligare harmonisera och effektivisera skyddet av personuppgifter i syfte att förbättra den inre marknadens funktion och öka enskildas kontroll över sina personuppgifter. Enligt kommissionen kommer förslaget att undanröja den fragmentariska dataskyddsreglering som nu finns inom EU, vilket både förenklar för företagen och stärker den enskildes rätt till skydd för sina personuppgifter. Eftersom regleringen föreslås få formen av en förordning blir den direkt tillämplig i medlemsstaterna när den trätt i kraft.

Förslaget till uppgiftsskyddsförordning baseras till stor del på den struktur och reglering som finns i det nu gällande dataskyddsdirektivet. Den föreslagna förordningen är liksom dataskyddsdirektivet utformad enligt en hanteringsmodell som innebär att själva hanteringen av personuppgifter regleras från det att uppgifterna samlas in till dess att de utplånas. Förordningen innehåller dock även en rad nyheter jämfört med dataskyddsdirektivet.

3.3.2 Förslaget till uppgiftsskyddsförordning

Syfte och tillämpningsområde

I förordningens första kapitel slås syftet och tillämpningsområdet fast, vilka är i princip desamma som dataskyddsdirektivets (artiklarna 1–3). Det territoriella tillämpningsområdet utvidgas dock till att även omfatta uppgiftsbehandling som sker utanför EU så länge behandlingen utförs av företag som t.ex. erbjuder varor eller tjänster till EU-medborgare.

I kapitlet finns också en rad definitioner av begrepp som används i förordningen (artikel 4). Många av definitionerna motsvarar vad som gäller enligt dataskyddsdirektivet men vissa av definitionerna har ändrats och andra har tillkommit, t.ex. definitioner av personuppgiftsbrott samt genetiska och biometriska uppgifter. Defi-

nitionen av samtycke har ändrats på så sätt att ett samtycke alltid måste vara uttryckligt för att det ska anses utgöra ett giltigt samtycke i förordningens mening.

Principer och krav på behandlingen av personuppgifter

Det andra kapitlet innehåller de principer som ska styra behandlingen av personuppgifter. Principerna motsvarar i stora drag de som redan gäller enligt dataskyddsdirektivet vad gäller t.ex. rättsliga grunder för behandling och behandling av känsliga personuppgifter. En nyhet är införandet av en princip om att behandling av personuppgifter måste ske på ett öppet sätt (artikel 5). Det slås vidare fast att behandling efter en intresseavvägning inte kan åberopas som rättslig grund vid myndigheters behandling av personuppgifter i deras myndighetsutövning (artikel 7.1 f). En ytterligare nyhet är att en registeransvarig inte är skyldig att skaffa fram ytterligare information för att kunna identifiera en registrerad enbart för att kunna iaktta någon bestämmelse i förordningen (artikel 10).

Den enskildes rättigheter

Det tredje kapitlet innehåller bestämmelser om den enskildes rättigheter. Först och främst slås fast att den registeransvarige ska ha tydliga och lättillgängliga riktlinjer och vara skyldig att ge klar och tydlig information till den enskilde vad gäller behandlingen av personuppgifter samt informera mottagare av uppgifter under vissa villkor (artiklarna 11–13). Den enskildes rätt till information bygger i stor utsträckning på direktivets bestämmelser. I likhet med vad som redan gäller har den registrerade också rätt att få felaktiga uppgifter rättade samt att få ofullständiga uppgifter kompletterade (artiklarna 14–16).

Den nuvarande rätten att få uppgifter raderade vidareutvecklas genom förordningen till att även avse en rätt att bli ”glömd”. Detta innebär att den registeransvarige inte endast ska radera personuppgifter som inte längre får behandlas. Om uppgifterna har gjorts offentliga ska den registeransvarige dessutom vidta alla rimliga åtgärder för att informera dem som uppgifterna spridits till att den

enskilde vill bli glömd. En begäran om att få bli glömd innebär som huvudregel att uppgifterna ska raderas utan dröjsmål. Endast i vissa särskilt uppräknade undantagsfall får uppgifter behållas trots den enskildes begäran om att bli glömd (artikel 17).

I förordningen införs också en rätt för den enskilde att få en kopia av de personuppgifter som behandlas samt en rätt att få personuppgifter överförda från en registeransvarig, t.ex. en tjänsteleverantör, till en annan, s.k. dataportabilitet (artikel 18).

Kapitlet innehåller vidare bestämmelser som vidareutvecklar nu gällande reglering om den enskildes rätt att invända mot uppgiftsbehandling och att i viss utsträckning inte bli utsatt för s.k. profilering, dvs. automatisk behandling av uppgifter i syfte att bedöma personliga egenskaper hos den enskilde som exempelvis arbetsprestationer eller kreditvärdighet (artiklarna 19 och 20).

Slutligen ges medlemsstaterna befogenhet att för vissa särskilt uppräknade ändamål inskränka vissa av rättigheterna och skyldigheterna i förordningen genom nationell lagstiftning. En förutsättning för att få införa sådana inskränkningar är dock att de är nödvändiga och proportionella i förhållande till det eftersträvade ändamålet (artikel 21). Bestämmelsen motsvarar artikel 13 i dataskyddsdirektivet.

Skyldigheter för den som behandlar personuppgifter

Det fjärde kapitlet i förordningen innehåller bestämmelser om vilka skyldigheter som den registeransvarige och den som behandlar uppgifterna för dennes räkning, dvs. registerföraren (personuppgiftsbiträdet enligt personuppgiftslagen) har.

Även om många av skyldigheterna har motsvarigheter i dataskyddsdirektivet innebär förslaget att skyldigheterna utökas och vidareutvecklas. Exempelvis fastställs den registeransvariges skyldigheter som följer av principerna om inbyggt uppgiftsskydd och uppgiftsskydd som standard (artikel 23). Således ska den personuppgiftsansvarige, både i samband med att det bestäms hur behandlingen ska utföras och vid tidpunkten för själva behandlingen, vidta åtgärder för att säkerställa att kraven i förordningen uppfylls (”data protection by design”). Den registeransvarige ska även säkerställa att behandlingen, som standard, endast får avse de personuppgifter

som är nödvändiga i förhållande till syftet med behandlingen (”data protection by default”).

Vidare klargörs gemensamma registeransvarigas ansvar vad gäller förhållandena dem emellan och gentemot den registrerade (artikel 24).

Registerförarens ställning och skyldigheter regleras avsevärt mera utförligt i förordningen än i dataskyddsdirektivet (artikel 26). Exempelvis klargörs att en registerförare som behandlar andra uppgifter än de som anges i den registeransvariges instruktioner ska anses som gemensamt registeransvarig. Över huvud taget följer av flera bestämmelser i förordningen ett medansvar för registerförare som är nytt i förhållande till dataskyddsdirektivet. Exempelvis kan även en registerförare bli skadeståndsskyldig gentemot den registrerade vid otillåten behandling (artikel 77).

Den registeransvarige och registerföraren är vidare skyldig, på liknande sätt som gäller enligt direktivet, att vidta lämpliga säkerhetsåtgärder för att skydda de personuppgifter som behandlas (artikel 30). Det införs också en skyldighet för den registeransvarige att utan dröjsmål, om möjligt inom 24 timmar, underrätta tillsynsmyndigheten om ett inträffat personuppgiftsbrott, t.ex. ett dataintrång (artikel 31). I vissa fall krävs det även att de enskilda som berörs av personuppgiftsbrottet underrättas (artikel 32).

Den registeransvarige ska dessutom i vissa fall låta göra en konsekvensanalys avseende integritetsriskerna med en planerad uppgiftsbehandling (artikel 33). Den generella skyldigheten enligt dataskyddsdirektivet att anmäla behandling av personuppgifter till den nationella tillsynsmyndigheten har tagits bort. Enligt förordningen ska det endast finnas anmälningsskyldighet och krav på förhandstillstånd i fråga om personuppgiftsbehandling som innebär särskilda risker (artikel 34). I stället ska det föras och bevaras en detaljerad dokumentation om den uppgiftsbehandling som genomförs (artikel 28). Denna dokumentation ska efter begäran göras tillgänglig för tillsynsmyndigheten.

Varje myndighet samt alla företag med minst 250 anställda eller vars huvudsakliga verksamhet är sådan att den kräver regelbunden övervakning av enskilda ska även utse ett uppgiftsskyddsombud. Uppgiftsskyddsombudet ska utses för en period om minst två år och ges möjlighet att på ett självständigt sätt övervaka att myndigheten eller företaget uppfyller förordningens krav (artiklarna 35–37).

Överföring av uppgifter till länder och internationella organisationer utanför EU

I förordningens femte kapitel regleras under vilka förutsättningar personuppgifter får överföras till tredjeland eller till en internationell organisation utanför EU. Den föreslagna regleringen innebär en vidareutveckling av motsvarande reglering i dataskyddsdirektivet. Liksom enligt direktivet är det ett grundläggande krav för sådan överföring att det mottagande tredjelandet säkerställer en adekvat skyddsnivå för uppgifterna. I regel är det kommissionen som ska besluta om ett tredjeland uppfyller detta krav eller inte (artiklarna 40 och 41). Om kommissionen har beslutat att ett tredjeland inte har en adekvat skyddsnivå så innebär detta ett förbud för överföring av uppgifter dit. Har kommissionen inte fattat något beslut i frågan finns det möjlighet att överföra uppgifter till tredjeland om vissa juridiskt bindande skyddsåtgärder vidtas, som t.ex. användandet av vissa godkända standardavtalsklausuler, eller med stöd av vissa direkta undantag (artikel 42–44).

Tillsynsmyndigheter

I det sjätte kapitlet finns bestämmelser om den nationella tillsynsmyndigheten. Reglerna påminner i stort om regleringen i dataskyddsdirektivet. Tillsynsmyndigheten ges dock vissa nya skyldigheter och befogenheter, som t.ex. en skyldighet att pröva klagomål om uppgiftsbehandling och en befogenhet att väcka talan i domstol vid överträdelser mot bestämmelserna i förordningen (artikel 52). Genom förslaget införs också en befogenhet för de nationella tillsynsmyndigheterna att besluta om administrativa sanktionsavgifter (artikel 53).

Tillsynsmyndigheternas samarbete och åtgärder för en konsekvent tillämpning

Genom bestämmelserna i det sjunde kapitlet i förordningen (artiklarna 55–72) införs uttryckliga regler om tillsynsmyndigheternas samarbete över nationsgränserna. Vidare föreslås en särskild mekanism som ska garantera att förordningen tillämpas på ett konse-

kvent sätt i hela EU. För att uppnå detta syfte ska det bland annat inrättas en europeisk dataskyddsstyrelse bestående av representanter för de nationella dataskyddsmyndigheterna. Dataskyddsstyrelsen ersätter Arbetsgruppen för uppgiftsskydd, den s.k. Artikel 29-gruppen, som tillskapats enligt dataskyddsdirektivet. De nationella tillsynsmyndigheterna är skyldiga att samråda med dataskyddsstyrelsen innan de vidtar någon åtgärd som kan få effekter i flera medlemsstater. Dataskyddsstyrelsen ska i sådana fall utfärda ett yttrande som den nationella tillsynsmyndigheten måste ta hänsyn till. Även kommissionen ges rätt att utfärda sådana yttranden som den nationella tillsynsmyndigheten måste beakta.

Rättsmedel, ansvar och sanktioner

Bestämmelserna i det åttonde kapitlet bygger på och utvecklar motsvarande reglering i dataskyddsdirektivet. I kapitlet slås fast att enskilda ska ha rätt att klaga hos en nationell tillsynsmyndighet om de anser att behandlingen av deras personuppgifter inte följt regleringen i förordningen (artikel 73).

Den enskilde ska dessutom ges rättsmedel för att kunna få tillsynsmyndigheten att agera utifrån ett klagomål som framförts till myndigheten (artikel 74). I likhet med vad som redan gäller ska den enskilde även ha rätt att väcka talan vid domstol mot en registeransvarig. En nyhet är att rätten gäller även gentemot en registerförare (artikel 75).

Om en enskild har drabbats av en skada på grund av en otillåten behandling av personuppgifter ska denne ha rätt till skadestånd från den som är ansvarig för behandlingen, den registeransvarige eller registerföraren (artikel 77). I övrigt är det medlemsstaterna som ska fastställa de sanktioner som ska komma i fråga vid överträdelser av förordningens bestämmelser. Sanktionerna måste dock vara effektiva, proportionerliga och avskräckande (artikel 78). En nyhet är att de nationella tillsynsmyndigheterna är skyldiga att besluta om administrativa sanktionsavgifter vid vissa överträdelser av förordningen. De belopp som ska dömas ut anges i förordningen och kan uppgå till en miljon euro, eller två procent av ett företags globala omsättning, vid de allvarligaste överträdelserna av förordningens bestämmelser (artikel 79).

Behandling av personuppgifter för vissa särskilda ändamål

I det nionde kapitlet finns bestämmelser om behandling av personuppgifter för vissa särskilda ändamål. För att skapa en balans mellan skyddet för personuppgifter och yttrandefriheten anges exempelvis att medlemsstaterna ska lagstifta om undantag från vissa av förordningens bestämmelser för sådan behandling av personuppgifter som sker uteslutande för journalistiska ändamål eller för konstnärligt eller litterärt skapande (artikel 80). Det finns även särskilda bestämmelser som närmare reglerar behandling av uppgifter om hälsa samt behandling för statistiska, historiska eller vetenskapliga forskningsändamål (artikel 81 respektive 83). Medlemsstaterna får även lagstifta om sådan behandling av enskildas personuppgifter som har samband med anställning (artikel 82).

Kommissionens rätt att utfärda delegerade akter och genomförandeakter

En betydelsefull skillnad i förhållande till dataskyddsdirektivet är att kommissionen i ett stort antal bestämmelser i förordningen föreslås ges rätt att anta delegerade akter och genomförandeakter. Det handlar exempelvis om att utfärda rättsakter som närmare specificerar innebörden av vissa krav som enligt förordningen ställs på behandling av uppgifter samt rätt att utfärda olika standardformulär och procedurregler som ska gälla vid tillämpningen av förordningen. Bestämmelserna i det tionde kapitlet reglerar de närmare villkoren för dessa delegerade befogenheter.

Ikraftträdande m.m.

Det elfte kapitlet innehåller förordningens avslutande bestämmelser. Det föreslås bland annat att kommissionen ska utvärdera förordningen och rapportera till ministerrådet och Europaparlamentet. Förordningen ska enligt förslaget börja tillämpas två år efter att den offentliggjorts (artikel 91).

3.3.3 Förhandlingsarbetet

Europaparlamentet

I Europaparlamentet behandlas dataskyddsreformen i utskottet för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor (LIBE-utskottet). Rapportören för uppgiftsskyddsförordningen, Jan Philipp Albrecht, lade fram ett förslag till betänkande i december 2012 och den 22 oktober 2013 röstade LIBE-utskottet fram ett förslag. Den 12 mars 2014 antog Europarlamentet en resolution efter en omröstning som resulterade i en mycket stark majoritet för förslaget till uppgiftsskyddsförordning, 621 ja-röster, 10 nej-röster och 22 nedlagda röster. Förslaget till direktiv för den brottsbekämpande verksamheten antogs med 371 ja-röster, 276 nej-röster och 30 nedlagda röster.

I resolutionen beträffande uppgiftsskyddsförordningen har Europaparlamentet föreslagit ett flertal ändringar och tillägg. Generellt föreslår parlamentet ett betydligt snävare utrymme för kommissionen att anta delegerade akter och genomförandeakter.

LIBE-utskottet, med rapportören Jan Philipp Albrecht, är även efter parlamentets resolution och EU-valet våren 2014 ansvarigt för uppgiftsskyddsförordningen i parlamentet. Något nytt ställningstagande har emellertid inte gjorts efter valet utan man avvaktar att rådet ska bli klart med sina förhandlingar.

Ministerrådet

Alltsedan år 2012 har uppgiftsskyddsförordningen förhandlats i Rådet för rättsliga och inrikes frågor, RIF-rådet. Förhandlingarna pågår fortfarande. Hittills har emellertid tre delöverenskommelser uppnåtts.

Redan initialt i förhandlingarna om förordningen framkom att det tycktes föreligga relativt stor enighet inom rådet om att det finns behov av att skapa ytterligare flexibilitet för den offentliga sektorn. Detsamma gällde även för behovet av att införa en mer riskbaserad ansats. Vid ett möte i RIF-rådet i juni 2013 infördes efter förslag från bl.a. Sverige en särskild artikel om tillgång till allmänna handlingar. Vid RIF-rådet i juni 2014 träffades en överenskommelse om partiell allmän inriktning när det gäller förordningens

kapitel V, som innehåller bestämmelser om överföring av personuppgifter till länder och internationella organisationer utanför EU och EES. Vid RIF-rådet i oktober 2014 träffades en överenskommelse om partiell allmän inriktning när det gäller kapitel IV, som främst innehåller bestämmelser om de personuppgiftsansvarigas skyldigheter. Vid det senaste mötet i december 2014 uppnåddes en överenskommelse om partiell allmän inriktning med ändringar i artiklarna 1(2)a, 6(3) och 21 och hela kapitel 9. De aktuella ändringarna i bestämmelserna reglerar hur förordningens regelverk förhåller sig till nationella regleringar om den offentliga sektorn och vilket utrymme medlemsstaterna ska ha att i vissa situationer och vid viss personuppgiftsbehandling anta specifika, och även i vissa fall avvikande, bestämmelser i förhållande till förordningens regelverk. Syftet med ändringarna är att skapa ytterligare flexibilitet för den offentliga sektorns behandling av personuppgifter.

Vad händer nu?

Den fortsatta processen med uppgiftsskyddsförordningen är alltså beroende av att förhandlingarna inom rådet kan slutföras. EU:s nuvarande ordförandeland, Lettland, har som ambition att RIF-rådet i juni 2015 ska kunna besluta om en allmän inriktning om hela uppgiftsskyddsförordningen, dvs. rådets förslag till förordningstext. Det förslaget kommer sedan att vara utgångspunkten för rådets förhandlingar, trilogen, med Europaparlamentet och kommissionen om uppgiftsskyddsförordningen. Europeiska rådet (stats- och regeringscheferna) har ställt i utsikt att man bör kunna nå fram till en överenskommelse mellan institutionerna under 2015.

Ett införande av förordningen har bedömts viktigt för att förverkliga ambitionen om en ”digital inre marknad” (Digital Single Market), vilken är av pelarna i den gällande digitala agendan för EU samt också en prioriterad fråga i kommissionens arbetsprogram för 2015. Ambitionen synes således vara att lagstiftningsprocessen ska drivas med inriktning på ett slutförande och ett beslut om införande av förordningen inom en inte alltför avlägsen tid. Enligt kommissionens förslag ska uppgiftsskyddsförordningen börja tillämpas två år efter offentliggörandet. Europaparlamentet har inte föreslagit

någon ändring därvidlag och frågan har, såvitt framkommit, inte blivit föremål för någon delöverenskommelse inom rådet.

4 Registerförfattningar – ett komplext rättsområde

Vårt övergripande uppdrag är alltså att se över den s.k. registerlagstiftningen. I denna översyn ingår att göra en översiktlig inventering av gällande registerförfattningar. I detta kapitel redovisar vi i huvuddrag våra iakttagelser från inventeringen av registerförfattningarna. Vi redogör också för några generella problem med registerförfattningarna, dels sådana som framförts i tidigare sammanhang, dels sådana som vi själva identifierat i vårt arbete.

Kapitlet inleds med en beskrivning av framväxten av den i Sverige etablerade regleringsmodellen på persondataskyddsområdet som innebär att grundläggande regler ges i en generellt tillämplig lag och att specifika undantag eller andra särbestämmelser tas in i sådana särskilda lagar eller förordningar som kommit att kallas registerförfattningar.

4.1 Bakgrund

4.1.1 Registerförfattningarna och datalagen

Viss registerföring som i dag är reglerad i registerförfattningar har lång historik. Lantmäteriets fastighetsregister och Skatteverkets folkbokföring är ett par exempel på förande av förteckningar med månghundraåriga anor. Det har även förekommit författningsreglering av registerföring under lång tid i den meningen att det i författning föreskrivits att vissa register med visst innehåll ska föras och med en närmare reglering av registerverksamheten. Exempelvis har den nuvarande lagen (1998:620) om belastningsregister föregångare i lagen om allmänt kriminalregister från år 1963 som i sin tur föregicks av lagen om straffregister från år 1900. Det som

emellertid i dag kallas registerförfattningar har sin bakgrund i samhällets tilltagande datorisering under 1900-talets senare hälft och den integritetsdebatt som följde i spåren på denna utveckling.

Redan på 1960-talet började datoriseringens inverkan på samhället debatteras i många länder. Till en början handlade den svenska debatten om teknikens inverkan på offentlighetsprincipen. Det var emellertid 1970 års folk- och bostadsräkning som kom att spela rollen av utlösande faktor för en allmän debatt i Sverige om automatisk databehandling (ADB) och dess användning för personregistrering. Myndigheternas insamlande av uppgifter om människor och deras levnadsförhållanden ansågs öka myndigheternas makt och möjlighet att styra enskildas handlingar. Även försäljningen av personuppgifter från myndigheter till enskilda, som sedan användes för selektiv reklam, utsattes för häftig kritik. År 1971 fick Offentlighets- och sekretesslagstiftningskommittén i uppdrag att behandla frågan om lagstiftning rörande personorienterad ADB-information. Kommittén kom därmed att bli den första integritetsutredningen på dataområdet.

Offentlighets- och sekretesslagstiftningskommittén bedömde att ADB-teknikens utveckling, innebärande att stora mängder information kan föras samman i en enda enhet och därur göras analyser och sammanställningar, medförde nya faror för otillbörliga intrång i den personliga integritetssfären (SOU 1972:47 s. 56 ff.). Kommittén framhöll att det inte bara var betydelsefullt att förhindra reella risker för otillbörliga intrång. Beaktas borde även de psykologiska effekterna som vetskapen om ADB-användningen medförde med åtföljande behov hos enskilda av att kunna lita på att det privata området verkligen respekterades av myndigheter och organisationer. I detta sammanhang påtalades dock att rädslan för missbruk av datalagrad information inte fick undanskymma det förhållandet att ADB-teknikens utökade användning också hade haft mycket positiva effekter, både för samhällsekonomin och för samhällsplaneringen i stort.

Någon enhetlig definition av vad som avses med personlig integritet fanns inte då och finns inte heller i dag. Begreppet har uppmärksammats i flera statliga utredningar och blivit föremål för en del ingående analyser och attitydundersökningar (se bl.a. SOU 2007:22 s. 52 f. och 77 f.). Offentlighets- och sekretesslagstiftningskommittén hänvisade som bakgrund till sina överväganden

om en lagstiftning rörande personorienterad ADB-information till det i amerikansk juridisk doktrin utbildade rättsliga begreppet ”privacy” (SOU 1972 s. 56 f.). Grundtanken med begreppet är att den enskilde bör ha tillgång till en fredad sektor inom vilken han eller hon kan avvisa sådan inblandning både från det allmänna och från andra som uppfattas som otillbörlig. Rätten att bli lämnad i fred kan dock aldrig vara absolut i ett samhälle. Samhällets krav på insatser från den enskilde i fråga om t.ex. arbete och skatter måste begränsa den privata sektorn. Att närmare ange innehållet i den fredade sektorn ansåg Offentlighets- och sekretesslagstiftningskommittén vara svårt att göra, bl.a. eftersom man måste räkna med att det som bör skyddas efterhand kommer att förskjutas. Fakta om begångna brott, sjukdomar, mottagen socialhjälp angavs som exempel på typfall av information som det är ofrånkomligt att vissa myndigheter måste registrera för att uppfylla sina arbetsuppgifter, men som ur den enskildes synpunkt upplevs som ömtålig. Även enskildas åsikter gavs som exempel på ömtålig information. Kommittén underströk att inte bara vilken typ av information som avsågs var av betydelse utan även insamlande och hantering av ett stort antal i och för sig banala uppgifter kunde i samband med ADB-teknikens möjligheter medföra negativa konsekvenser för den personliga integriteten (a.a. s. 60). Spridning och fortsatt användning var också av stor betydelse.

Offentlighets- och sekretesslagstiftningskommittén bedömde att det fanns ett nära samband mellan anspråket på en fredad sektor och kravet från enskilda att bli bedömda efter relevanta kriterier. Om man vet att en myndighet har tillgång till omfattande information om enskildas personliga förhållanden ligger det nära till hands, menade kommittén, att misstänka att informationen utnyttjas till ställningstaganden som den inte är avsedd för. Vidare föreligger risk att ofördelaktiga uppgifter om en persons förflutna i otillbörlig grad kommer att påverka hans eller hennes möjligheter i framtiden. Samhällets krav på solidaritet och ekonomisk effektivitet måste därför begränsas, bl.a. genom att övervakningen av den enskilde inte tillåts bli fullständigt effektiv (SOU 1972:47 s. 63 f.).

Kommittén konstaterade att det system av befintliga skyddsregler som fanns genom bl.a. bestämmelserna om offentlighet- och sekretess och vissa straffbestämmelser, t.ex. brott mot post- och telehemlighet, var användbart mot integritetsintrång vid manuell

informationsbehandling. Däremot ansågs dessa bestämmelser komma till korta gentemot den automatiska databehandlingen. Särskilda regler för att möta det nya hotet ansågs därför påkallade. För att komma till rätta med riskerna med ADB-teknikens utveckling och de därmed sammanhängande riskerna för otillbörliga intrång i den personliga integriteten avseende registrering av personuppgifter lade kommittén fram ett förslag till en datalag. Förslaget ledde till genomförandet av den numera upphävda datalagen (1973:289).

Datalagen och statsmaktsregister

Datalagens syfte var att hindra att hanteringen av ADB-förda personregister medförde otillbörliga intrång i den personliga integriteten. Registrering skulle få förekomma, men det krävdes att vissa regler iakttogs. Lagen var tillämplig inom både den offentliga och privata sektorn och byggde på ett tillståndssystem. Enligt lagens ursprungliga lydelse krävdes – med visst undantag – tillstånd av den då nyinrättade Datainspektionen för att starta eller föra ett personregister med ADB. Detta gällde register hos såväl myndigheter som privata aktörer. Tillståndskravet kom senare att i vissa fall ersättas av ett anmälningsförfarande. Utöver tillstånd förutsattes Datainspektionen meddela föreskrifter om registrets ändamål, vilka personuppgifter som fick ingå samt, vid behov, föreskrifter om bl.a. inhämtandet av personuppgifter, tillåtna ADB-bearbetningar, utlämnande av personuppgifter, bevarande och gallring eller kontroll och säkerhet.

Offentlighets- och sekretesslagstiftningskommittén hade föreslagit att Datainspektionens tillståndsprövning även skulle omfatta personregister vars inrättande beslutats av statsmakterna, dvs. av riksdagen eller regeringen. I motiven till datalagen uttalade emellertid departementschefen att det av flera skäl torde vara nödvändigt att särbehandla vissa statliga personregister och anförde vidare följande (prop. 1973:33 s. 97).

> För det första bör riksdagen kunna besluta om inrättande av personregister för riksdagens egen verksamhet eller verksamheten hos organ som är underställt riksdagen. Vidare förekommer på den offentliga sektorn personregistrering av sådan vikt från allmän och enskild synpunkt att det är nödvändigt att frågan om registrens inrättande förbehålls statsmakterna själva. Ofta ges föreskrifter för registrering i form av lag

eller annan författning som meddelas av riksdagen och Kungl. Maj:t eller endera av dem. Exempel på register av denna typ finns bl.a. på rättsväsendets område.

Från datalagens krav på tillstånd kom alltså personregister vars inrättande beslutats av riksdagen eller regeringen, s.k. statsmaktsregister, att undantas (2 § datalagen, sedermera 2 a §). Enligt motiven gällde undantaget oberoende av om beslutet om registrets inrättande gavs formen av lag eller annan författning eller kom till uttryck på annat sätt (prop. 1973:33 s. 97). Innan sådant beslut fattades skulle dock yttrande inhämtas från Datainspektionen. När Datainspektionen avgav ett sådant yttrande skulle en bedömning av registret ske enligt samma grunder som vid prövning av ett tillståndsärende. Datainspektionen kunde även meddela föreskrifter för registret i den mån riksdagen eller regeringen inte hade gjort det, t.ex. om ändamål eller bevarande och gallring. Dessutom omfattades även statsmaktsregister av Datainspektionens tillsyn enligt datalagen.

För övriga personregister som en kommunal eller statlig myndighet kunde inrätta krävdes tillstånd från Datainspektionen. När det gällde personregister som innehöll uppgifter om bl.a. straffprocessuella eller administrativa frihetsberövanden eller någons sjukdom eller hälsotillstånd, dvs. registrering av uppgifter som bedömdes vara av särskilt känslig natur, infördes dock särskilda restriktioner för att tillstånd till registerföringen skulle kunna medges annan än myndighet som enligt lag eller annan författning hade att föra förteckning över sådana uppgifter (4 § datalagen). Indirekt förutsattes alltså redan vid datalagens tillkomst att förandet av personregister med särskilt integritetskänsligt innehåll hade uttryckligt författningsstöd. Det kan påpekas att det redan innan datalagens tillkomst fanns författningar med enstaka bestämmelser om t.ex. gallring, inhämtande och spridande av uppgifter i register som motiverades av hänsyn till de registrerades integritet. Exempel på sådana registerförfattningar var lagen (1963:197) om allmänt kriminalregister och lagen (1965:94) om polisregister. I huvudsak handlade dock äldre registerlagar om att ett register av visst innehåll skulle föras för att tillgodose något allmännyttigt syfte eller liknande. Det primära målet i dessa äldre författningar var således inte att värna om integriteten.

Några förarbetsuttalanden från datalagens tid

Även efter datalagens införande fortsatte datoranvändningen och den personliga integriteten att debatteras i samhället och nya utredningar tog vid efter Offentlighets- och sekretesslagstiftningskommittén.

Datalagstiftningskommittén fick 1976 uppdraget att göra en översyn av bl.a. datalagen. I sitt delbetänkande Personregister – datorer – integritet (SOU 1978:54) behandlade kommittén bl.a. frågor om samkörning av olika personregister och användning av personnummer (s. 85–112). I detta sammanhang redogjorde kommittén för de risker för otillbörligt intrång i den personliga integriteten som kan uppkomma genom att uppgifter som ursprungligen samlats in för ett ändamål senare används för ett annat ändamål. Ett sådant utnyttjande ansågs i otillbörlig grad minska den enskildes möjligheter att överblicka hur uppgifter som den enskilde själv en gång lämnat kan komma att användas. Även information som var harmlös i sig ansågs kunna innebära intrång i den enskildes integritet eftersom sammanställningar från olika register kunde leda till en kartläggning av en persons enskilda förhållanden. Likaså påtalades risken för utlämnande av den enskilde individen. Vidare framfördes farhågor om att det vid samkörning av register kunde vara svårt att kontrollera att uppgifterna var korrekta och aktuella. Därutöver aktualiserades mera abstrakta integritetsintrång, t.ex. att bara vetskapen om att de uppgifter man lämnat till en myndighet överförs mellan olika register kunde väcka obehag.

Datalagstiftningskommittén konstaterade att samkörningsfrågor alltmer aktualiserades vid myndigheternas handläggning av ansökningar från enskilda om behovsprövade förmåner och inom skatteadministrationen (a.a. s. 108 f.). Enligt kommittén väckte det frågor om vilka metoder att kontrollera enskildas uppgifter som var acceptabla. Intressekonflikten mellan behovet av effektiva kontroller och enskildas krav på personlig integritet medförde dock svåra avvägningsproblem. Hur intresseavvägningen skulle utfalla kunde dock inte en gång för alla slås fast genom en regel i datalagen. Det var snarare en fråga som måste avgöras från fall till fall grundade på politiska överväganden. Enligt kommittén var det väsentligt att beslut om inrättandet och användandet av offentliga personregister, som gav en djupare inblick i enskilda medborgares privata förhåll-

anden, fattades av riksdag eller regering och inte av de myndigheter som skulle använda registren. Detta borde gälla även ifråga om användning av register för nya ändamål. Över huvud taget förordade kommittén att ändamålen för statliga register angavs så tydligt som möjligt av riksdag eller regering samt att det skulle klargöras att registren inte fick användas för andra ändamål utan medgivande av riksdag eller regering. Kommittén uttalade vidare följande (a.a. s. 110).

> En metod att göra detta är att, såsom ibland redan skett, reglera registren genom lagar eller förordningar och att därvid meddela så långt möjligt uttömmande föreskrifter om användningen. Man bör alltså var för sig på ett i vart fall något sånär enhetligt sätt författningsreglera alla statliga register av betydelse i sammanhanget. Om det därefter uppkommer behov av att använda registren för andra syften än de som ursprungligen var aktuella får sådana behov prövas och avgöras från fall till fall enligt samma ordning. DALK [Datalagstiftningskommittén] förordar denna lösning.

Även Data- och offentlighetskommittén behandlade i delbetänkandet Integritetsskyddet i informationssamhället 4 (SOU 1987:31 s. 157 f.) frågor om samkörning, personnummeranvändning samt författningsreglering av personregister. I en kartläggning av personregistreringen konstaterade kommittén att register i en del fall har stöd i lag eller annan författning men att dessa ofta var föråldrade, t.ex. därför att de skapats för manuell registerhantering, eller saknade mera detaljerad reglering. Vidare var det mindre vanligt med författningar som beslutats av riksdagen (a.a. s. 47). Enligt kommittén måste målsättningen vara att personregister som är särskilt känsliga från integritetssynpunkt regleras av riksdagen i syfte att stärka skyddet av enskilda registrerades integritet. Beslut om ny eller utökad personregistrering föregås då av ordentlig utredning av konsekvenserna från integritetssynpunkt, vilket är av betydelse för att en reell intresseavvägning ska kunna göras. De register som särskilt utpekades var socialstyrelsens register, landstingens register, kommunernas register inom socialtjänsten och skolhälsovården samt Riksförsäkringsverkets och försäkringskassornas register. Vidare anfördes att Datainspektionen fortlöpande borde vara uppmärksam på om ytterligare register behöver specialreglering i lag. Om helt nya register som omfattar stora delar av befolkningen och innehåller integritetskänsliga uppgifter skapas i framtiden borde dessa

alltid lagregleras redan från början, menade kommittén. När det gällde frågan om lagstiftningsteknik anförde kommittén bl.a. följande (a.a. s. 159).

> Vi har övervägt möjligheten att sammanföra alla registerförfattningar under ett paraply. En sådan lösning skulle medverka till enhetlig utformning av lagstiftningen och ge utrymme för såväl behövlig modernisering av befintliga författningar som en ny reglering på de områden där sådan behövs. I en gemensam registerlag blir det emellertid svårt att reglera sådana centrala frågor som de olika registrens ändamål och innehåll. Det är också troligt att en för alla specialreglerade register gemensam registerlag blir alltför svåröverskådlig för att fylla sitt syfte. En möjlighet vore att ge registerlagen karaktären av ramlag och att komplettera med registerförordningar eller föreskrifter från DI [Datainspektionen] för varje enskilt register. En sådan ramlag skulle t.ex. kunna innehålla föreskrifter om vilka frågor som skall regleras i olika registerförfattningar. I princip ger dock datalagen redan vägledning på den punkten. Denna lösning ger också riksdagen mindre inflytande än vad som har varit fallet vid tillkomsten av befintliga registerlagar.

Data- och offentlighetskommittén stannade således för att fortsatta särförfattningar var att föredra samt att sådana skulle ges i lagform i fråga om register med kvalificerat känsliga personuppgifter som får en extern spridning som inte är obetydlig. Dock varnades för registerlagar utformade efter mall. I varje enskilt fall, framhöll kommittén, krävs en noggrann och individuell prövning. En registerlag som enbart syftar till att fungera som ett alibi för att verksamheten är under kontroll löser inte integritetsproblemen menade kommittén (SOU 1987:31 s. 161 f.).

Data- och offentlighetskommitténs överväganden kom att i den fortsatta framväxten av registerlagstiftningen få stor betydelse. I det efterföljande lagstiftningsarbetet anslöt sig regeringen liksom konstitutionsutskottet till kommitténs tankar om lämplig normgivningsnivå och gjorde uttalanden som ofta åberopats i senare lagstiftningsärenden som vägledande för att välja lagform för registerförfattningsreglering (prop. 1990/91:60 s. 58 och KU 1990/91:11 s. 11).

Under 1990-talet tillkom, mot bakgrund av nyss nämnda lagstiftningsärende, allt fler registerlagar. Det finns fortfarande registerlagar i kraft som tillkom som särlagstiftning i förhållande till datalagen. Lagen (1996:1156) om receptregister är ett exempel.

4.1.2 Registerförfattningarna och personuppgiftslagen

Dataskyddsdirektivets genomförande

Dataskyddsdirektivets genomfördes i svensk lagstiftning genom personuppgiftslagen. Personuppgiftslagen trädde i kraft den 24 oktober 1998 och ersatte då datalagen. Som har framgått är personuppgiftslagen till skillnad från datalagen teknikoberoende i den meningen att den i fråga om automatiserad behandling inte begränsas till dataregister. All automatiserad behandling omfattas, alltså även personuppgifter som framgår av bild eller ljud. Det avgörande är att personuppgifterna är föremål för automatiserad behandling, inte om de är ordnade i ett register eller inte. Till skillnad från datalagen innehåller personuppgiftslagen vidare inget krav på tillstånd för inrättande och förande av personregister. I stället innehåller lagen en rad hanteringsregler för behandling av personuppgifter.

Liksom datalagen utgör personuppgiftslagen emellertid en generellt tillämplig reglering som gäller för såväl myndigheter som enskilda vilka behandlar personuppgifter. I motiven till personuppgiftslagen diskuterades om lagens tillämpningsområde borde begränsas i några avseenden, bl.a. till att enbart omfatta verksamheter som omfattas av unionsrätten. En sådan begränsning ansågs dock strida mot vad som tillämpats under lång tid i Sverige, nämligen ett system som utgår från en generell lag kompletterad med särregler i s.k. registerförfattningar för viktigare och känsligare register. Personuppgiftslagen är därför generellt tillämplig och omfattar även verksamheter som faller utanför unionsrättens område (prop. 1997/98:44 s. 40 f.).

Av 2 § PuL följer vidare att om det i en annan lag eller förordning finns bestämmelser som avviker från lagen, ska de bestämmelserna gälla. Det är således endast särregler i lag eller förordning som tar över bestämmelserna i personuppgiftslagen. Inte bara särbestämmelser i registerförfattningar avses i 2 §. Även bestämmelser i andra slags lagar och förordningar om t.ex. uppgiftsskyldighet gäller före bestämmelserna i personuppgiftslagen (prop. 1997/98:44 s. 116).

Fortsatt särreglering i registerförfattningar

I motiven till personuppgiftslagen (prop. 1997/98:44 s. 40 f.) anförde regeringen bl.a. följande.

> Registerförfattningarna innehåller många preciserade och viktiga regler som inte rimligen kan ersättas av de generella bestämmelser som den nya lagen innehåller. Samtidigt står det klart att det är nödvändigt med särregler i förhållande till den nya lagen på flera viktiga områden, t.ex. beträffande polisens verksamhet. Frågan är därför om det redan i den nya lagen skall göras undantag för vissa verksamheter eller om nödvändiga särregler för dessa verksamheter liksom hittills skall ges i särskilda författningar som får gälla framför den nya lagen. […].
>
> Vi anser att det traditionella svenska systemet med särregler i särskilda författningar är att föredra framför generella undantag från den nya lagen. Det är i stort sett bara verksamhet inom den offentliga sektorn som med hänsyn till EG-direktivet skulle kunna undantas från den nya lagen. Inom den sektorn förekommer det t.ex. ofta stora mängder känsliga uppgifter och uppgifter som har hämtats in med stöd av straffsanktionerad uppgiftsplikt. Därför är det särskilt viktigt med ett starkt integritetsskydd när det gäller uppgifter inom all offentlig verksamhet. Om viss offentlig verksamhet skulle generellt undantas från lagen, finns det risk för att viss behandling inom den sektorn inte kommer att omfattas av någon lagstiftning med motsvarande syfte som den nya lagen. Genom att det krävs en särskild författning för att avvika från det integritetsskydd som den nya lagen ger, garanteras däremot att behovet av särregler alltid övervägs noga i den ordning som gäller för författningsgivning. Målet har också varit att myndighetsregister med ett stort antal registrerade och ett särskilt känsligt innehåll skall regleras särskilt i lag (prop. 1990/91:60 s. 50 och KU 1990/91:11 s. 11). Det finns inte anledning att nu avvika från det målet.
>
> Den nya lagen bör således vara generellt tillämplig och omfatta även sådan verksamhet som faller utanför EG-rätten samtidigt som avvikande bestämmelser i lag eller förordning skall gälla framför den nya lagen. Detta innebär också att den nya lagen i princip bara bör innehålla generella regler och att behovet av undantag och särregler för mer speciella områden får tillgodoses genom andra författningar.
>
> Såsom Datalagskommittén och flera remissinstanser har påpekat krävs det en anpassning av befintliga registerförfattningar och en översyn av vilka särregler som bör gälla i förhållande till den nya lagen. Vi avser att snarast påbörja ett sådant anpassnings- och översynsarbete.

Under övergångsperioden fram till den 30 september 2001 då personuppgiftslagen trädde i full kraft antogs ett flertal nya registerförfattningar som kom till genom den i motiven aviserade översynen. Vissa av dessa hade en annorlunda utformning jämfört med den som varit vanlig i tidigare registerförfattningar. Denna nya typ av registerförfattning har inte begränsats till att reglera viss personregisterföring utan särreglerar automatiserad personuppgiftsbehandling i viss verksamhet alldeles oavsett om den sker i register eller liknande informationssamlingar.

Offentlig verksamhet som inte är registerförfattningsreglerad

Det finns emellertid många myndigheter vars verksamhetsrelaterade personuppgiftsbehandling bara regleras genom personuppgiftslagen och inte särskilt i någon registerförfattning. Hur stor andel av den offentliga sektorns samlade personuppgiftsbehandling som inte är särreglerad är svårt att kvantifiera men så mycket står klart att den ”icke särreglerade” personuppgiftsbehandlingen sammantaget är omfattande.

På det statliga området finns t.ex. en förhållandevis stor mängd förvaltningsmyndigheter, i vart fall mer än hundratalet, som till övervägande del enbart tillämpar personuppgiftslagen i den behandling av personuppgifter som verksamheten föranleder. Till den kategorin hör stora myndigheter såsom universitet och högskolor. Visserligen finns särregler om viss registerföring över studieresultat, antagningsförhållanden m.m. i förordningen (1993:1153) om redovisning av studier m.m. vid universitet och högskolor, men det är ingen heltäckande författning för den behandling av personuppgifter som förekommer inom området och som inte bara avser studerande utan också exempelvis forskningspersoner vars personuppgifter, med eller utan den personens informerade samtycke, används inom ramen för olika forskningsprojekt eller studentarbeten.

Många statliga myndigheter som saknar registerförfattningar är jämförelsevis små men kan behöva hantera ganska känslig information i sin verksamhet. Inspektionen för vård- och omsorg, som bedriver tillsyn över hälso- och sjukvården och socialtjänsten och till vilken enskilda kan göra anmälningar om klagomål på vården m.m. liksom Ersättningsnämnden, som är tillfälligt inrättad för att han-

tera vissa anspråk på ersättning för vanvård av fosterbarn, samt Diskrimineringsombudsmannen är exempel på sådana myndigheter. Exempel på mycket små myndigheter som knappast torde ha anledning att behandla personuppgifter annat än i klart begränsad omfattning är Nämnden för hemslöjdsfrågor och Lagrådet.

På det kommunala området är skolverksamheten ett område som i stort sett saknar särreglering i förhållande till personuppgiftslagen men som sammantaget medför omfattande personuppgiftsbehandlingar. Hit hör både ärendehantering och faktisk verksamhet som skolmyndigheter ansvarar för och som bl.a. sker inom förskolan, fritidshemmen, grund- och gymnasieskolan och kommunal vuxenutbildning.

Kommunerna är vidare skyldiga enligt lag att bedriva vissa verksamheter t.ex. rörande stadsplanering och byggfrågor, renhållning, räddningstjänst och biblioteksverksamhet vilka alla föranleder viss personuppgiftsbehandling. Även kommunernas frivilliga verksamhet med kultur- och fritidsverksamhet kan nämnas som exempel på verksamhet där personuppgiftslagen tillämpas fullt ut.

4.2 Vår inventering av registerförfattningarna

4.2.1 Allmänt

Registerförfattningar förekommer både i form av lag och förordning.

Som har framgått har det länge varit en ambition att särskilt integritetskänslig registerföring ska regleras i lag, främst därför att en sådan normgivningsnivå borgar för att det görs en grundlig utredning och en ingående avvägning mellan integritetsintresset och de intressen som talar för registerföringen. Detta har gällt alldeles oavsett att lagform inte har varit nödvändig från rent normgivningsteknisk utgångpunkt. Det har emellertid framhållits att man inte har varit helt konsekvent vad gäller valet av normgivningsnivån i det översyns- och anpassningsarbete som inleddes i samband med personuppgiftslagens införande (Öman/Lindblom, s. 33).

Ganska ofta kompletteras en registerlag med en förordning som innehåller utfyllande bestämmelser. Vidare är det inte ovanligt att registerförfattningar innehåller bemyndiganden för utpekade myndigheter att meddela föreskrifter med närmare bestämmelser i vissa

frågor eller bestämmelser om undantag i olika avseenden. Myndighetsföreskrifter är alltså en tredje förekommande normgivningsnivå.

Vi har i enlighet med uppdraget enligt våra direktiv gjort en översiktlig inventering av gällande registerförfattningar. En inledande fråga vi ställde oss var hur många sådana författningar det finns. Den frågan kan förefalla vara enkel att besvara men vi har funnit att så inte är fallet. Svaret är nämligen helt beroende av hur man väljer att avgränsa begreppet registerförfattning, vilket är en komplex fråga. Är det t.ex. en registerförfattning bara därför att en myndighet åläggs att föra ett visst register oavsett om detta innehåller personuppgifter eller inte eller ska bara författningar med bestämmelser rörande ett register där vissa personuppgifter kan förekomma omfattas av begreppet?

Ett exempel på en svårklassificerad författning är förordningen (2011:93) om stöd till insatser på livsmedelsområdet som föreskriver att Jordbruksverket ska föra ett register över stödmottagare. Det sägs inget om att registret får eller inte får föras elektroniskt och specifika bestämmelser om dataskydd saknas helt. Samma förhållande gäller för det centrala passregistret som Polismyndigheten ska föra enligt passförordningen (1979:664).

Det finns vidare många författningar vars enda inslag av dataskyddsreglering är att ange att personuppgiftslagens bestämmelser om skadestånd och rättelse gäller även för informationshantering enligt författningen i fråga eller att det föreskrivs ett undantag från personuppgiftslagens grundläggande förbud mot överföring av personuppgifter till tredje land. Det finns också exempel på författningar där det finns enstaka bestämmelser om personuppgiftsbehandling, vilka dock inte riktar sig till myndigheter utan till enskilda aktörer, se t.ex. 6 kap. 1–8 §§ lagen (2010:751) om betaltjänster. Vidare finns författningar som innehåller bestämmelser om personuppgiftsbehandling men som helt saknar reglering av registerföring som sådan.

Av huvudsakligt intresse för vårt arbete är regler om persondataskydd vid helt eller delvis elektronisk informationshantering hos myndigheter. Vi har därför valt att i vårt arbete låta begreppet registerförfattning omfatta författningar som i något avseende innehåller särbestämmelser i förhållande till eller hänvisningar till personuppgiftslagen alldeles oavsett om författningen i fråga rör registerföring eller inte. Den avgränsningen tycks också stå bäst i

överensstämmelse med den allmänna uppfattningen rörande vad som numera utmärker en registerförfattning. Enbart det förhållandet att en viss registerföring regleras i en författning innebär alltså inte att författningen nödvändigtvis är att se som en registerförfattning i nu aktuell mening.

Det är alltså regler av dataskyddsrättslig natur, dvs. bestämmelser som avser att skydda enskildas personliga integritet, och som är föranledda av ett behov av att avvika från eller komplettera det integritetsskydd som personuppgiftslagen annars ger som vi haft som främsta urvalskriterium när vi gjort vår inventering. Med detta kriterium omfattas både sådana bestämmelser som syftar till ge författningsstöd åt en personuppgiftsbehandling som inte hade varit tillåten enligt personuppgiftslagen, t.ex. utökade möjligheter att behandla känsliga personuppgifter, eller som syftar till att i förhållande till personuppgiftslagen begränsa myndigheternas möjligheter att behandla personuppgifter t.ex. genom att endast tillåta registrering av vissa slags personuppgifter.

Initialt har vi gått till väga på det viset att vi gjort sökningar i rättsdatabaser med användande av olika sökord för att få fram författningar som kan utgöra särregleringar i förhållande till personuppgiftslagen. Exempelvis har vi använt sökbegrepp såsom ”$register”, ”$registret”, ”personuppgift$”, ”databas”, ”direktåtkomst”, ”sökbegr$”, gallr$” m.fl. begrepp, för separat sökning eller i kombinationer.

Resultatet av våra sökningar bildar en brokig karta av författningar i form av lagar eller förordningar som sinsemellan företer mer eller mindre stora likheter och olikheter, även efter det att alla träffar som helt saknar intresse för utredningsuppdraget sorterats bort. Bland bortsorterade författningar ingår dels sådana som helt saknar bestämmelser om behandling av personuppgifter eller annan reglering av dataskyddskaraktär, dels sådana som enbart reglerar förhållanden hos enskilda aktörer.

4.2.2 Tre kategorier registerförfattningar

Vi har valt att sortera de författningar som vi har bedömt vara att betrakta som registerförfattningar i tre någorlunda avgränsade kategorier, nämligen som endera a) renodlade registerförfattningar,

b) informationshanteringsförfattningar och c) annan reglering med inslag av dataskyddsbestämmelser. Vi har däremot inte sett det som meningsfullt att kategorisera författningarna utifrån normhierarkisk nivå, dvs. som lagar respektive förordningar eller utifrån olika sakliga verksamhetssektorer exempelvis såsom rörande statlig respektive kommunal verksamhet osv. Det ska dock framhållas att våra sorteringskategorier är ganska trubbiga och att många författningar skulle kunna bedömas falla inom mer än en kategori.

Renodlade registerförfattningar

Den första kategorin registerförfattningar utmärks av att tillämpningsområdet endast avser inrättandet, förandet och användningen av något enstaka register eller annan bestämd informationssamling. En del sådana registerförfattningar är förhållandevis gamla, ett exempel är förordningen (1970:517) om rättsväsendets informationssystem, men det tillkommer fortlöpande nya författningar av detta slag. Förordningen (2014:885) om register över vigselförrättare, som förs av Kammarkollegiet, är ett sådant exempel.

Renodlade registerförfattningar handlar ofta om register som enligt statsmakterna ska föras och som ska ha ett visst obligatoriskt innehåll. Genom en sådan registerförfattning åläggs en myndighet att föra ett visst register, registerföringen blir alltså genom författningsregleringen en del i myndighetens uppdrag. Den verksamhetsreglering som registerförfattningen därigenom kan sägas avse kringgärdas emellertid ofta av dataskyddsreglering som syftar till att garantera enskilda registrerade ett skydd för deras personliga integritet i hanteringen av personuppgifter i samband med registerföringen. Lagen (2001:558) om vägtrafikregister med anknytande förordning är ett exempel härpå. Det finns dock exempel på författningar i denna kategori där anslaget är ett annat genom att det regleras att register får, inte ska, föras eller vad de får innehålla, se t.ex. lagen (1998:543) om hälsodataregister med anslutande förordningar för specifika hälsodataregister (t.ex. för Socialstyrelsens patientregister, cancerregister, läkemedelsregister m.fl.). Det hör dock till bilden att det i praktiken oftast tycks vara underförstått att sådana register som det talas om att myndigheter får föra, faktiskt också ska föras. Detta kan t.ex. framgå av föreskrifter om

skyldigheter för andra aktörer att inrapportera vissa uppgifter till den registerförande myndigheten. En skillnad mellan författningar som föreskriver att register ska föras i förhållande till sådana som talar om att register får föras är att de senare normalt har en tydligare prägel av att utgöra dataskyddsreglering snarare än verksamhetsreglering.

Vi har identifierat uppemot ett 70-tal författningar som vi hänfört till kategorin renodlade registerförfattningar. I de allra flesta fall är det fråga om förordningar. I de fall sådana författningar har lagform så har i allmänhet åberopats riksdagens och regeringens ställningstagande i början av 1990-talet om att myndighetsregister med ett stort antal registrerade och ett särskilt känsligt innehåll bör regleras särskilt i lag i syfte att stärka skyddet för de registrerades integritet. Exempel på detta är lagen om vägtrafikregister och lagen (2009:619) om djurskyddskontrollregister (prop. 2000/01:95 s. 55 och prop. 2008/09:143 s. 18 f.). Av nyare datum är lagen (2012:453) om register över nationella vaccinationsprogram (vaccinationsregistret). I motiven till den sistnämnda lagen motiverades lagformen för registret med att det därigenom upprättades ett starkare skydd för hanteringen av data som är av stor betydelse för den personliga integriteten (prop. 2011/12:123 s. 67).

Variationerna inom sorteringskategorin renodlade registerförfattningar är emellertid stora. I ganska många författningar spelar den dataskyddande regleringen inte någon särskilt framträdande roll i jämförelse med den verksamhetsreglering som författningarnas bestämmelser i övrigt ger uttryck för, t.ex. i fråga om anmälnings- eller ansökningsförfaranden och i fråga om att det finns kataloger över vilka uppgifter som ska registreras. Exempel härpå är författningar för de s.k. publicitetsregistren som har till syfte att förse allmänheten med information om vissa förhållanden, t.ex. rörande aktiebolag, fordon, patent m.m., och där registreringen i sig medför vissa rättsverkningar. Dock är det vanligt att det såvitt avser personuppgifter finns bestämmelser om registrets ändamål, personuppgiftsansvar, sökbegränsningar, direktåtkomst, utlämnande på medium för automatiserad behandling, rättelse och skadestånd samt gallring. Det kan också finnas bestämmelser om t.ex. vilka avgifter som får eller ska tas ut vid utlämnande av uppgifter och handlingar i elektronisk form.

Ett antal renodlade registerförfattningar har emellertid en tydlig prägel av att i allt väsentligt utgöra en dataskyddsreglering, dvs. där inslaget av verksamhetsreglering m.m. inte dominerar utan där det framgår att syftet med regleringen är att ge mer preciserade eller avvikande bestämmelser i förhållande till personuppgiftslagen. Den nyss nämnda lagen om register över nationella vaccinationsprogram är ett exempel på en sådan författning liksom lagen om hälsodataregister. Andra exempel är lagen om receptregister och lagen (2013:794) om vissa register för forskning om vad arv och miljö betyder för människors hälsa. Denna typ av registerförfattningar ligger till struktur och innehåll relativt nära det vi kallar informationshanteringsförfattningar. En skillnad gentemot informationshanteringsförfattningarna är dock att registerförfattningar av detta sistnämnda slag genomgående konstruerats så att det uttryckligen anges att personuppgiftslagen gäller i den mån registerförfattningen i fråga inte innehåller avvikande bestämmelser. I registerförfattningar som främst syftar till att reglera en viss verksamhet, nämligen att bedriva ett visst register, förekommer däremot att förhållandet till personuppgiftslagen inte berörs alls. I sak torde detta dock inte innebära någon egentlig skillnad.

Vissa myndigheters verksamheter är till stor del knutna till och styrda av renodlade registerförfattningar, t.ex. verksamheten hos Lantmäteriet (fastighetsregistret, pantbrevsregistret, lägenhetsregistret m.fl.), Bolagsverket (aktiebolagsregistret, handelsregistret m.fl.) och Transportstyrelsen (vägtrafikregistret m.fl.) För andra myndigheter är registerförfattningar om förandet av vissa register mindre styrande för verksamheten som helhet, t.ex. för Finansinspektionen (insiderregistret, krigsskaderegistret m.fl.) eller Jordbruksverket (djurskyddskontrollregistret m.fl.). Mellanformer finns där tillämpning av registerförfattningar dominerar delar av en myndighets verksamhet såsom t.ex. är fallet med Socialstyrelsens verksamhet med hälsodataregister.

Som tidigare berörts är det inga vattentäta skott mellan de sorteringskategorier som vi använder oss av. Ett exempel på detta är förordningen (2001:720) om behandling av personuppgifter i verksamhet enligt utlännings- och medborgarskapslagstiftningen. Den reglerar Migrationsverkets, Polismyndighetens, Säkerhetspolisens och utlandsmyndigheternas personuppgiftsbehandling i verksamhet enligt den nämnda lagstiftningen. Förordningen reglerar en

mycket omfattande personuppgiftsbehandling hos myndigheterna men är enligt sin ordalydelse begränsad till att reglera vissa register, verksamhetsregister samt Migrationsverkets rättsfallsregister, fingeravtrycksregister samt landinformationsregister. Förordningen företer emellertid i realiteten starka drag av informationshanteringsförfattning.

Informationshanteringsförfattningar

Den andra sorteringskategorin började förekomma i samband med personuppgiftslagens införande. Dessa författningar har som övergripande funktion att utöver eller i stället för personuppgiftslagen särreglera personuppgiftsbehandling i stort inom vissa utpekade verksamheter eller myndigheter. Här handlar det alltså inte bara om att viss registerföring ska eller får ske. Oftast omfattar regleringen såväl registerföring, ärendehanteringssystem eller andra strukturerade personuppgiftssamlingar liksom annan slags behandling utan koppling till ärendehanteringssystem, exempelvis behandling i löpande text. I och med att tillämpningsområdet är vidare än att enbart reglera personuppgifter i register är det i egentlig mening missvisande att kalla dem för registerförfattningar men uttryckssättet har levt kvar och kommit att omfatta även denna kategori författningar.

Utmärkande för denna kategori är att de i huvudsak reglerar vilken personuppgiftsbehandling myndigheter får utföra inom ramen för författningens tillämpningsområde. Inte sällan finns dock särbestämmelser rörande vissa register, databaser eller gemensamt tillgängliga uppgiftssamlingar som får eller ska finnas i den aktuella myndighetens verksamhet.

Informationshanteringsförfattningar har i allmänhet form av lag som kompletteras av förordningar med närmare bestämmelser. Det finns också fristående förordningar som är att betrakta som informationshanteringsförfattningar. Så är t.ex. fallet när det gäller nu gällande registerförfattningar på domstolarnas område respektive inom åklagarväsendet.

Till kategorin informationshanteringsförfattningar har vi, med bortseende från den brottsbekämpande sektorn, bl.a. hänfört följande författningar.

- Lagen (1998:938) om behandling av personuppgifter om totalförsvarspliktiga med förordning, gäller för Totalförsvarets pliktverk
- Lagen (2001:181) om behandling av uppgifter i Skatteverkets beskattningsverksamhet med förordning
- Lagen (2001:182) om behandling av personuppgifter i Skatteverkets folkbokföringsverksamhet med förordning
- Lagen (2001:183) om behandling av personuppgifter i verksamhet med val och folkomröstningar med förordning, gäller för Valmyndigheten
- Lagen (2001:184) om behandling av uppgifter i Kronofogdemyndighetens verksamhet med förordning
- Lagen (2001:185) om behandling av uppgifter i Tullverkets verksamhet med förordning
- Lagen om behandling av personuppgifter inom socialtjänsten (2001:454) med förordning, gäller för kommunala myndigheter, Statens Institutionsstyrelse samt enskilda aktörer
- De s.k. Veraförordningarna (2001:639–642), gäller för domstolarna och hyres- och arrendenämnderna
- Lagen (2002:546) om behandling av personuppgifter inom den arbetsmarknadspolitiska verksamheten med förordning, gäller för Arbetsförmedlingen
- Lagen (2006:469) om behandling av personuppgifter vid Inspektionen för arbetslöshetsförsäkringen med förordning
- Lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst med förordning
- Lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet med förordning
- Patientdatalagen (2008:355) med förordning, gäller för kommunala och landstingskommunala hälso- och sjukvårdsmyndigheter och andra sorters myndigheter som bedriver hälso- och sjuk-

vård, t.ex. inom skolhälsovård, Kriminalvården, Försvarsmakten, Statens institutionsstyrelse m.fl. Lagen gäller även för enskilda vårdgivare.

- Studiestödsdatalagen (2009:287) med förordning, gäller för Centrala studiestödsnämnden
- Förordningen (2011:306) om behandling av personuppgifter i Tandvårds- och läkemedelsförmånsverkets verksamhet i fråga om det statliga tandvårdsstödet
- Kustbevakningsdatalagen (2012:145) i den mån lagen avser annat än brottsbekämpning, gäller för Kustbevakningen
- Lagen (2012:741) om behandling av personuppgifter vid Institutet för arbetsmarknads- och utbildningspolitisk utvärdering med förordning

Även när det gäller denna sorteringskategori förekommer relativt stora variationer. Något som har varit särskilt omdiskuterat genom åren är att författningarna systematiskt har utformats på olika sätt när det gäller förhållandet till personuppgiftslagen. Även ändamålsbestämmelser har utformats på olika sätt och begrepp har använts med delvis olika innebörd m.m.

Dock finns även många likheter. Särskilt gäller detta vilka slags frågor som i allmänhet regleras i författningarna, nämligen frågor om tillämpningsområde, varvid det förekommer föreskrifter om att vissa bestämmelser ska gälla även vid hantering av uppgifter om avlidna eller juridiska personer, personuppgiftsansvar, tillåtna ändamål för dels insamling och myndighetens egen användning av personuppgifter (primära ändamål) dels tillhandahållande av personuppgifter till externa mottagare (sekundära ändamål), vilka personuppgifter som får behandlas, betydelsen av den registrerades inställning till behandlingen, sökbegrepp, specifika hanteringsregler för register, databaser eller andra uppgiftssamlingar, säkerhetfrågor såsom begränsningar av tillgången till lagrade personuppgifter, direktåtkomst och annat elektroniskt utlämnande, bevarande och gallring samt frågor om rättelse, skadestånd och överklagande. Detaljeringsgraden varierar emellertid betydligt. Vissa författningar har mer har karaktären av ramlagar med generella bestämmelser, t.ex. patientdatalagen med anknytande förordning, medan andra har en jäm-

förelsevis detaljerad reglering rörande bl.a. vilka uppgifter om vilka kategorier av personer som får behandlas, t.ex. lagen om behandling av personuppgifter inom den arbetsmarknadspolitiska verksamheten med anknytande förordning.

På de områden där det finns mer eller mindre heltäckande informationshanteringsförfattningar för berörda myndigheters verksamhet brukar det indirekt av de beskrivna tillämpningsområdena och genom förarbetsuttalanden framgå att myndigheternas personal- och ekonomiadministration inte omfattas av regleringen i fråga. I den verksamheten ska i stället personuppgiftslagen tillämpas. Ett exempel härpå är 1 § studiestödsdatalagen enligt vilken lagen ska tillämpas vid behandling av personuppgifter i Centrala studiestödsnämndens studiestödsverksamhet. I motiven har beskrivits vad som närmare avses med studiestödsverksamheten. Vidare har angetts att behandling av personuppgifter som sker inom ramen för myndighetens interna administration inte omfattas av lagen (prop. 2008/09:96 s. 33 f.).

Det kan ibland förekomma ytterligare särreglering av viss personuppgiftsbehandling inom en myndighet parallellt med sådan mer övergripande särreglering av myndighetens personuppgiftsbehandling genom en informationshanteringsförfattning. Exempel härpå är Skatteverkets verksamheter med äktenskapsregistret respektive med identitetskort för folkbokförda i Sverige som omfattas av särskilda registerförordningar samt med verksamheten rörande förmedlingen av elektroniska försändelser från myndigheter till enskilda i e-tjänsten Mina meddelanden (förordningen [1987:1022] om äktenskapsregistret, förordningen [2009:284] om identitetskort för folkbokförda i Sverige samt förordningen [2003:770] om statliga myndigheters elektroniska informationsutbyte).

Annan reglering med inslag av dataskyddsbestämmelser

Den tredje sorteringskategorin är med vårt synsätt egentligen inte registerförfattningar alls. Till den kategorin hör olika slags författningar som inte syftar till att främst reglera ett visst register eller annan behandling av personuppgifter, utan bara till en mindre del innehåller bestämmelser som rör personuppgiftsbehandling och i den delen utgör särreglering i förhållande till personuppgiftslagen.

Sådan reglering kan t.ex. gälla förandet av ett visst register. Exempel härpå är bestämmelser om viss registerföring i skogsvårdslagen (1979:429), vapenlagen (1996:67), konkurslagen (1987:672), biobankslagen (2002:297) och alkohollagen (2010:1622). Det kan också handla om författningar med enstaka undantag från personuppgiftslagens bestämmelser, t.ex. i fråga om förbudet mot att överföra personuppgifter till tredjeland såsom i lagen (2012:318) om 1996 års Haagkonvention. Den lagen hänvisar även till användningsbegränsningar i konventionen ifråga.

Vi har identifierat mer än ett hundratal författningar som hör till denna kategori. Men vi utesluter inte att det finns ytterligare författningar som är av det här slaget. Vi har t.ex. bortsett från sådana författningar som bara i något visst hänseende har relevans för myndigheters personuppgiftsbehandling t.ex. författningar som föreskriver olika slags uppgiftsskyldigheter eller förfaranderegleringar. En författning av sistnämnt slag är rättegångsbalken som kan sägas innehålla en specifik reglering av dataskyddande karaktär i 27 kap. 24 § som avser bevarande respektive förstöring av upptagningar från hemliga tvångsmedel.

Myndigheter såsom exempelvis Centrala studiestödsnämnden, Försäkringskassan och Pensionsmyndigheten är statistikansvariga myndigheter rörande officiell statistik och har i den verksamheten att följa de särregler om behandling av personuppgifter som följer av lagen (2001:99) om officiell statistik med anknytande förordning. Den sistnämnda lagen och förordningen tillhör den kategori författningar som väsentligen utgör verksamhetsreglering men där det finns vissa regler om personuppgiftsbehandling som gäller för statistikansvariga myndigheter. Vad beträffar t.ex. Försäkringskassan och Centrala studiestödsnämnden omfattas sakverksamheten av annan särreglering men så är dock inte alltid fallet, t.ex. i fråga om Brottsförebyggande rådet eller Tillväxtverket. Det kan nämnas att det oftast är förutsatt att statistikansvariga myndigheters verksamhet med den officiella statistiken ska vara en självständig verksamhetsgren inom sådana myndigheter som bedriver annan huvudsaklig verksamhet än statistikverksamhet.

Lagen (1998:112) om ansvar för elektroniska anslagstavlor kan vidare nämnas i detta sammanhang eftersom den har betydelse för alla myndigheters verksamhet på sociala medier. Bland annat innehåller lagen särskilda skyldigheter att informera och gallra på myn-

dighetens egna sociala medier, t.ex. om myndigheten har en interaktiv chattfunktion på den egna webbplatsen. Detta torde utgöra en viss särreglering i förhållande till personuppgiftslagen trots att det inte tycks ha varit ett uttalat syfte med lagen. Här kan även nämnas 6 kap. 18 § lagen (2003:389) om elektronisk kommunikation enligt vilken den som tillhandahåller en webbplats är skyldig att informera om ändamålen med och inhämta samtycke till användningen av s.k. cookies. Det kravet gäller även för myndigheter.

Kameraövervakningslagen (2013:460) är en generellt tillämplig lag som uttryckligen gäller i stället för personuppgiftslagen – vad avser behandling av personuppgifter i ljud och bild – och som kan bli tillämplig hos alla myndigheter förutsatt att myndigheten bedriver sådan kameraövervakning med övervakningsutrustning som avses i lagen.

Registerförfattningar – ett rörligt rättsområde

Registerförfattningsbeståndet är i hög grad varierande även i det avseendet att det fortsatt tillkommer nya registerförfattningar med särregleringar för olika delar av den offentliga sektorn. Den anpassning och översyn av registerförfattningsområdet som vidtogs i samband med personuppgiftslagens införande har inneburit ett omfattande arbete som kan sägas fortfarande pågå. Det ligger i sakens natur att registerförfattningsbeståndet aldrig kan bli ”färdigt” eftersom den offentliga verksamheten genomgår ständiga förändringar.

Bland registerförfattningar som införts parallellt med vårt utredningsarbete kan nämnas lagen (2013:794) om vissa register för forskning om vad arv och miljö betyder för människors hälsa med anknytande förordning. Denna författning hör till kategorin renodlade registerförfattningar. Under år 2014 har vidare några författningar beslutats vari bestämmelser om vissa myndigheters personuppgiftsbehandling införts, nämligen lagen (2014:51) om infrastrukturavgifter på väg, som gäller viss registerföring m.m. hos Transportstyrelsen, och lagen (2014:105) om insyn i finansiering av partier, som medger Kammarkollegiet möjlighet att behandla känsliga personuppgifter som lämnats i en intäktsredovisning eller som annars är nödvändiga för att Kammarkollegiet ska kunna fullgöra

sina skyldigheter enligt lagen. Dessa båda sistnämnda lagar tillhör det slags författningar som vi kategoriserar som annan reglering med inslag av dataskyddsbestämmelser.

Som exempel på pågående lagstiftningsarbete kan nämnas 2014 års utlänningsdatautredning (Ju 2014:11) som har i uppdrag att utarbeta förslag till en lag om behandling av personuppgifter i verksamhet enligt utlännings- och medborgarskapslagstiftningen som ska ersätta förordningen (2001:720) om behandling av personuppgifter i verksamhet enligt utlännings- och medborgarskapslagstiftningen (dir. 2014:76).

4.3 En problembeskrivning

4.3.1 Tidigare kritik

De särskilda registerförfattningarna har på olika sätt kritiserats under ganska lång tid. Kritiken har riktats både mot systemet med registerförfattningar som sådant och mot brister i författningarnas konstruktion, val av begreppsapparat m.m. I våra direktiv anges som en bakgrund till vårt uppdrag att se över registerlagstiftningen att en sådan översyn har efterlysts av bl.a. flera utredningar. I det följande presenteras vissa synpunkter som har framförts tidigare i olika sammanhang.

Toppledarforum

Redan på datalagens tid påtalade Toppledarforum – ett samarbetsorgan som under mitten av 1990-talet sysslade med verksamhetsutveckling i offentlig verksamhet med stöd av informationsteknik – att systemet med registerförfattningar medförde vissa problem. Bland annat anfördes att författningsmetodiken var ologisk, omständlig och tidsödande. Vidare framhölls att systemändringar även av detaljkaraktär, t.ex. på grund av ändringar i en verksamhet eller den tekniska utvecklingen, ofta måste föregås av ändringar i registerförfattningar, vilket tar tid och kräver resurser inom riksdag, regeringen och den berörda myndigheten. Angelägna projekt försenas eller blir inte av. Behovet av befintliga registerförfattningar borde därför omprövas och nya registerförfattningar enligt den gamla

modellen borde inte införas, även om undantag kunde tänkas för mycket speciella verksamheter såsom säkerhetspolisen och delar av sjukvården (Toppledaforum, LEXIT – förstudie, 1995 s. 37 f.).

Massmedia

Journalistförbundet har i en framställan till regeringen (Ju2006/4517/L6) anfört att den omfattande regleringen i registerförfattningar medför att undersökningar av stora material försvåras eller omöjliggörs, vilket hotar medias möjligheter att granska hur makten utövas och förvaltas. Framställan gjordes bl.a. mot bakgrund av förbundets egen utredning Registerlagarna – den absoluta sekretessen (2006-04-19). Enligt förbundet är det främst registerförfattningarnas bestämmelser om sökförbud och begränsningar i fråga om utlämnande på medium för automatiserad behandling som har dessa effekter.

Offentlighets- och sekretesskommittén

I sitt huvudbetänkande Ny sekretesslag (SOU 2003:99) berörde Offentlighets- och sekretesskommittén förhållandet mellan sekretesslagstiftningen och förekomsten i registerförfattningar av bestämmelser om tillåtna ändamål för personuppgiftsbehandlingen. Enligt kommittén finns det oklarheter angående sambandet mellan registerförfattningar och den s.k. finalitetsprincipen enligt dataskyddsdirektivet när det gäller uppgiftslämnande mellan myndigheter.

Integritetsskyddskommittén

Integritetsskyddskommittén kritiserade registerförfattningarna på ett antal punkter i sitt delbetänkande Skyddet för den personliga integriteten (SOU 2007:22 s. 461 f.). Bland annat pekade kommittén på att den reformering av registerförfattningarna som har skett efter personuppgiftslagens ikraftträdande har skett utan egentlig samordning. Skiftande lagstiftningsteknik har använts för att reglera registerförfattningarnas förhållande till personuppgiftslagen. Det förekommer att olika begrepp används för att beskriva samma

företeelser. Exempelvis används begreppet databas i en del författningar, medan man i andra har hållit fast vid det sedan tidigare etablerade begreppet register. Det förekommer dessutom att samma begrepp används i olika betydelser i skilda författningar, t.ex. begreppet direktåtkomst som inte alltid avser utlämnande på elektroniskt medium. Vidare har skilda tekniker använts för att beskriva de ändamål för vilka verksamheten, och därigenom behandlingen av personuppgifter, bedrivs. I en del registerförfattningar har ändamålen delats upp i primära och sekundära registerförfattningar där de sistnämnda syftar till att bl.a. beskriva de ändamål för vilka uppgifter får lämnas ut från den aktuella verksamheten. Detta har i sin tur medfört att oklarheter har uppstått bl.a. om hur sådana bestämmelser förhåller sig till finalitetsprincipen. Dessa brister i samordning och enhetlighet har lett till oklarheter i tillämpningen och svårigheter att överblicka regelverket, vilket i sin tur innebär en risk för onödiga integritetsförluster.

Kommittén framhöll också att i den mån det finns bestämmelser i en registerförfattning som inskränker integritetsskyddet borde det framgå av reglerna vari inskränkningen består och hur stor den är. Så är dock inte alltid fallet. Ett exempel på detta var regleringen av direktåtkomst.

Enligt kommitténs sammanfattande analys skulle skyddet för den personliga integriteten väsentligt förbättras om registerförfattningarna utformades enhetligare, tydligare och mer i överensstämmelse med sekretesslagstiftningen.

2005 års informationsutbytesutredning

Även 2005 års informationsutbytesutredning riktade i sitt betänkande Utökat elektroniskt informationsutbyte (SOU 2007:45) kritik mot registerförfattningarna. Utredningen konstaterade att registerförfattningarna bör ses över för att skapa förutsättningar för ett samordnat och enhetligt regelverk som främjar utvecklingen av elektronisk förvaltning och minskar riskerna för oacceptabla intrång i den personliga integriteten. Utredningen anförde bl.a. följande (a. bet. s. 394).

> Begreppsbildningen på området är oklar och framtagen under en tid av helt andra och mer begränsade möjligheter till elektroniskt informationsutbyte. Dessa förhållanden skapar onödiga hinder för utveck-

lingen. Enligt vår mening är det en avgörande förutsättning för ett väl fungerande elektroniskt informationsutbyte och elektronisk förvaltning överhuvudtaget att det finns ett samordnat regelverk med enhetlig struktur för alla myndigheter, utan otydliga begrepp och andra onödiga hinder för önskvärd utveckling. Även från integritetsskyddssynpunkt medför den bristande strukturen i författningarna och den oklara begreppsbildningen tillämpningssvårigheter som innebär ökade risker för oacceptabla intrång i den personliga integriteten.

E-delegationen

E-delegationen föreslog i delbetänkandet Strategi för myndigheternas arbete med e-förvaltning (SOU 2009:86) att regeringen skulle tillsätta en utredning med uppdrag att göra en översyn av registerförfattningarna och lämna förslag till bestämmelser som är samordnade, enhetliga och tydliga och där det ingår att lämna förslag till hur regelkonflikter inom register- och sekretesslagstiftningen ska lösas. En sådan reform av registerförfattningarna krävs, påpekade E-delegationen, för att möjliggöra en utveckling i riktning mot en flexibel e-förvaltning. E-delegationen framhöll att i en elektronisk förvaltning måste olika intressen balanseras mot varandra, nämligen intresset av effektivitet, integritet och öppenhet. Dessa tre begrepp borde enligt E-delegationen vara ledord för översynen av registerförfattningarna (a. bet. s. 65 f.).

E-offentlighetskommittén

E-offentlighetskommittén hade bl.a. i uppdrag att överväga om det i sekretesslagstiftningen eller i annan lag skulle införas en skyldighet för myndigheter att lämna ut elektroniskt lagrade allmänna handlingar i elektronisk form. I sitt slutbetänkande Allmänna handlingar i elektronisk form – offentlighet och integritet (SOU 2010:4) gjorde kommittén bedömningen att det befintliga regelverket till skydd för den personliga integriteten i samband med utlämnande av allmänna handlingar inte säkerställer en godtagbar skyddsnivå i fråga om intrång i enskildas personliga integritet vid ett införande en elektronisk offentlighetsprincip. Den främsta orsaken till det var, menade kommittén, de brister som finns inbyggda i det omfattande regelverk som registerförfattningarna utgör (a. bet. s. 15 f. och 290 f.).

Det var framför allt två slags brister som påtalades. För det första konstaterade kommittén att registerförfattningars sökbegränsningar i vissa fall inte utformats på sätt som gjorde att de träffas av den s.k. begränsningsregeln i 2 kap. 3 § tredje stycket TF trots att avsikten torde ha varit att så skulle ske. De begränsningar som finns var dessutom svåra att överblicka. För det andra fann kommittén ett flertal brister eller oklarheter i registerförfattningars bestämmelser om utlämnande av allmänna handlingar i elektronisk form, i den mån sådana alls förekom. Enligt kommitténs bedömning fanns det troligen många fall där förbud mot elektroniskt utlämnande inte har ansetts motiverat, eller helt enkelt förbisetts, men där det i specifika fall inte borde ske utlämnande i elektronisk form (a. bet. s. 293). I övrigt instämde kommittén med de kritiska påpekanden som framförts av bl.a. Integritetsskyddskommittén och framhöll för egen del det angelägna i en allmän översyn av gällande registerförfattningar och av begreppsbildningen på området för att komma till rätta med de problem som regleringen innebär.

4.3.2 Några ytterligare iakttagelser

Vi återkommer i det följande till redan påtalade specifika problem liksom till problem som vi själva iakttagit och som hänger samman med den befintliga registerförfattningsregleringen.

Vi vill emellertid redan här framhålla att vår inventering av gällande registerförfattningar och vårt övriga arbete – bl.a. i form av kontakter med olika myndigheter och enskilda aktörer – har bekräftat bilden av registerlagstiftningen som ett svåröverblickbart och fragmenterat rättsområde. Redan begreppet registerförfattning, oavsett hur det avgränsas, är tvetydigt. Det som avses utgörs av en tämligen brokig samling författningar som spänner över disparata verksamhetsområden inom hela den offentliga sektorn.

Komplexiteten i regleringen är generellt sett hög, vilket bl.a. beror på att registerförfattningsregleringen bara är en del av det regelverk som styr en myndighets informationshantering. Parallellt med registerförfattningar måste myndigheterna även följa 2 kap. TF, sekretesslagstiftningen liksom förvaltningslagen, arkivlagstiftningen samt annan generell eller myndighetsspecifik reglering som direkt eller indirekt har betydelse för informationshanteringen. Som an-

förs i våra direktiv är det för effektiviseringen av förvaltningen med hjälp av modern informationsteknik viktigt dels att respektive regelverk är väl genomtänkt och så enkelt som möjligt att tillämpa, dels att dessa regelverk är förenliga med varandra. Det är emellertid uppenbart att en anpassning till andra parallella och för informationshanteringen centrala regelverk inte alltid getts tillräcklig uppmärksamhet i lagstiftningsarbetet. Resultatet är bl.a. förekomsten av överlappningar och verkliga eller uppfattade motstridigheter i regleringen vilket medför risk för tillämpningsproblem. Det upplevs dessutom förekomma glapp i regleringen utifrån de behov av informationshantering som finns, vilket leder till osäkerhet och därmed knappast främjar servicen eller effektiviteten i förvaltningen. Det sagda gäller både myndighetsintern informationshantering och vid olika slags informationsutbyten.

Komplexiteten i registerförfattningsregleringen beror emellertid också på inkonsekvenser i regeltekniska strukturer och begreppsanvändning m.m. Samarbeten som myndigheterna åläggs av statsmakterna kan försvåras av olikheter i registerförfattningar som inte är, eller i vart fall inte förefaller vara, kompatibla med varandra.

Till detta kommer att den befintliga regleringen – som alltså är svåröverskådlig redan för lagstiftare och tillämpare – för den enskilde registrerade torde framstå som i det närmaste ogenomtränglig. Möjligheten för den enskilde att kunna förstå vilka dataskyddsregler som styr informationshanteringen av uppgifter om honom eller henne hos respektive myndighet är central. Överskådlighet och begriplighet är viktiga komponenter för enskilda registrerade som vill göra gällande sina rättigheter enligt det dataskyddsrättsliga regelverket. Även i detta avseende finns uppenbara brister.

Den splittrade och ibland inkonsekventa regleringen försvårar också för allmänheten att sätta sig in i vad som gäller på olika områden, vilket är särskilt olyckligt när det handlar om utövandet av den grundlagsskyddade rätten till insyn i myndigheternas allmänna handlingar. Vi har t.ex. erfarit att det är ett problem vid s.k. vidareutnyttjande av offentlig information att det splittrade sättet att reglera myndigheters registerföring gör att det krävs resurser att sätta sig in i nya förutsättningar varje gång en ny myndighet ska kontaktas.

Utöver de problem med registerförfattningar som beskrivits ovan har vi i vårt arbete kunnat konstatera att det finns en särskild

problembild som hör samman med att den allmänna regleringen i personuppgiftslagen har utformats utan närmare hänsyn till de förhållanden som gäller för myndigheternas personuppgiftsbehandling. Personuppgiftslagen är väsentligen utformad som en civilrättslig reglering. För myndigheter i allmänhet, alltså inte bara sådana som omfattas av särskild registerförfattningsreglering, präglas personuppgiftsbehandlingen emellertid av att den sker i författningsreglerade verksamheter med skyldigheter för myndigheterna och rättigheter för enskilda. Personuppgiftslagen är dock – med vissa undantag – i grunden inte anpassad till detta.

SÄRSKILDA FRÅGOR

5 Bör en åtskillnad mellan olika former av elektroniskt utlämnande behållas?

5.1 Problembild enligt direktiven och utredningens delbetänkande

5.1.1 Direktiven

Vi ska överväga om det finns skäl att i registerförfattningar behålla åtskillnaden mellan olika former av elektroniskt utlämnande. Som bakgrund till uppdraget i denna del anförs bl.a. följande i våra direktiv. Den tekniska utvecklingen har inneburit att det numera finns betydligt fler sätt att överföra uppgifter elektroniskt än tidigare och att nya åtkomstmetoder alltjämt tillkommer. Detta har medfört att det uppfattas som oklart hur begreppen direktåtkomst och utlämnande på medium för automatiserad behandling ska tillämpas på modernare metoder för informationsutbyte. De aktuella begreppen används inte heller på ett enhetligt sätt i de olika registerförfattningarna och utöver nu nämnda begrepp förekommer andra, t.ex. ”elektronisk åtkomst”.

5.1.2 Utredningens bedömning i delbetänkandet

I delbetänkandet Överskottsinformation vid direktåtkomst (SOU 2012:90) uttalade vi att det står klart att begreppsapparaten vad avser reglering i registerförfattningar av elektroniska utlämnandeformer måste bli tydligare och vara enhetlig (s. 212 f.). Det finns således ett behov av reformer på området. Vi föreslog inte någon grundlagsändring i delbetänkandet i syfte att undanta överskottsinformation vid direktåtkomst från begreppet allmän handling.

Därför var det inte påkallat att redan i delbetänkandet, innan vårt arbete med en samlad översyn av registerlagstiftningen var klart, göra några slutgiltiga ställningstaganden eller lägga fram några konkreta förslag till ny regleringsmodell på området. Vi avsåg därför att återkomma till frågan i slutbetänkandet.

5.2 Nuvarande regler som i allmän mening styr uppgiftsutbyte mellan myndigheter

5.2.1 Samverkan enligt förvaltningslagen

Enligt 6 § FL, ska varje myndighet lämna andra myndigheter hjälp inom ramen för den egna verksamheten.

Ytterligare bestämmelser om samverkan mellan förvaltningsmyndigheter under regeringen finns i 6 § myndighetsförordningen (2007:515). Enligt stadgandets andra stycke ska en myndighet verka för att genom samarbete med myndigheter och andra ta till vara de fördelar som kan vinnas för enskilda samt för staten som helhet. Vidare sägs i tredje stycket att myndigheten ska tillhandahålla information om myndighetens verksamhet.

Utrymmet för samverkan mellan myndigheterna enligt de ovan nämnda bestämmelserna påverkas av innehållet i annan lagstiftning, exempelvis regler om sekretess. En samverkan får inte heller ta sig sådana former att de medverkande myndigheternas olika funktioner blandas samman och inte klart kan urskiljas (se JO 1993/94 s. 458).

5.2.2 Offentlighets- och sekretesslagen

I offentlighets- och sekretesslagen finns flera regler som påverkar möjligheterna för myndigheter att utbyta uppgifter med varandra. I vissa fall innebär dessa regler också rättigheter respektive skyldigheter för myndigheter vid sådant utbyte. Nedan redogörs för de regler i offentlighets- och sekretesslagen som har betydelse för ett uppgiftsutbyte, nämligen bestämmelser om informationsskyldighet, sekretess mellan myndigheter, i vilka fall sekretess bryts och överföring av sekretess.

Informationsskyldighet mellan myndigheter

Enligt 6 kap. 5 § OSL ska en myndighet på begäran av en annan myndighet lämna uppgift som den förfogar över, om inte uppgiften är sekretessbelagd eller det skulle hindra arbetets behöriga gång.

Bestämmelsen kan ses som en precisering av myndigheters skyldighet att samverka enligt 6 § FL. Den skyldighet att lämna information till andra myndigheter som bestämmelsen föreskriver avser varje uppgift som myndigheten förfogar över och alltså inte bara uppgifter ur allmänna handlingar. Skyldigheten är således mer vidsträckt än den som gäller gentemot allmänheten (Lenberg m.fl., kommentaren till 6 kap. 5 §).

I vissa fall kan en mer långtgående skyldighet att lämna uppgifter gälla gentemot andra myndigheter enligt särskilda föreskrifter, s.k. sekretessbrytande bestämmelser (jfr 10 kap. 15 § och 28 § första stycket).

Sekretess mellan myndigheter

Enligt 8 kap. 1 § OSL får en uppgift för vilken sekretess gäller enligt den lagen inte röjas för andra myndigheter, om inte annat anges i den lagen eller i lag eller förordning som lagen hänvisar till.

Av 8 kap. 2 § följer att vad som föreskrivs om sekretess mot andra myndigheter i 1 § och vad som föreskrivs i andra bestämmelser om uppgiftslämnande till andra myndigheter och överföring av sekretess mellan myndigheter, gäller också mellan olika verksamhetsgrenar inom en myndighet när de är att betrakta som självständiga i förhållande till varandra.

Bestämmelsen har sin motsvarighet i 2 kap. 8 § TF om när en handling blir allmän när den överlämnats mellan organ inom samma myndighetsorganisation. Det avgörande är även i detta fall att organen uppträder som självständiga i förhållande till varandra.

Frågan om när organ eller verksamhetsgrenar inom samma myndighetsorganisation är att betrakta som självständiga i förhållande till varandra kan vara svårbedömd. Den har diskuterats både i lagstiftningsarbetet (se exempelvis prop. 2007/08:126 s. 162 f. om kommunal hälso- och sjukvård) och i rättspraxis (HFD 2013 ref. 40) samt inom ramen för JO:s tillsyn (se exempelvis JO 1995/96 s. 431

om stöd och service till funktionshindrade kunde ses som en självständig verksamhetsgren i förhållande till socialtjänsten).

Sekretessbrytande bestämmelser

Enligt 12 kap. 2 § andra stycket OSL kan en enskild helt eller delvis häva sekretess som gäller till skydd för honom eller henne, om inte annat anges i den lagen. I 10 kap. 1 § samma lag erinras om att sekretess till skydd för enskild alltså inte hindrar att en uppgift lämnas till en annan enskild eller en myndighet, om den enskilde samtycker till det.

Av 10 kap. 2 § OSL följer att sekretess inte hindrar att en uppgift lämnas till en enskild eller en annan myndighet, om det är nödvändigt för att den utlämnande myndigheten ska kunna fullgöra sin verksamhet. Bestämmelsen bör tillämpas restriktivt (prop. 1979/80:2 Del A s. 465 och 494). Avsikten är inte att rena effektivitetsskäl ska utgöra tillräckliga skäl att bryta sekretessen. Det är ett behov hos den utlämnande myndigheten som kan utgöra skäl att bryta sekretessen, däremot inte att den mottagande myndigheten behöver uppgiften för sin verksamhet.

I 10 kap. 27 § OSL finns en bestämmelse, den s.k. generalklausulen, som enbart tar sikte på att i visst fall bryta sekretess mellan myndigheter. Den kan således inte tillämpas vid utlämnande till en enskild. Enligt bestämmelsen får en sekretessbelagd uppgift lämnas till en myndighet, om det är uppenbart att intresset av att uppgiften lämnas har företräde framför det intresse som sekretessen ska skydda. Viss sekretess har undantagits från bestämmelsens tillämpningsområde (se andra stycket), exempelvis sekretess inom hälso- och sjukvården och socialtjänsten.

Har det i lag eller förordning föreskrivits att uppgifter ”bör” eller ”får” lämnas från en myndighet till en annan, finns det särskild anledning att anse att generalklausulen är tillämplig. Riksdagens eller regeringens föreskrifter med en sådan innebörd bör ju vara grundade på den bedömningen att intresset av att ett uppgiftsutbyte sker har företräde framför sekretessintresset (Lenberg m.fl., kommentaren till 10 kap. 27 §). Även om utgångspunkten är att ett rutinmässigt uppgiftsutbyte ska vara författningsreglerat hindrar inte generalklausulen att sådant utbyte sker även utan stöd av en

särskild författningsreglering. I de undantagsfall när rutinmässigt uppgiftsutlämnande inte är författningsreglerat men likväl kan anses tillräckligt motiverat måste den intresseavvägning som ska göras enligt generalklausulen ske på förhand och behöver inte avse en prövning i enskilda fall (prop. 1979/80:2 Del A s. 326).

Om det finns förutsättningar att lämna ut en sekretessbelagd uppgift med stöd av generalklausulen är den myndighet som förvarar uppgiften enligt 6 kap. 5 § OSL skyldig att lämna ut den.

I 10 kap. 28 § första stycket OSL stadgas att sekretess inte hindrar att en uppgift lämnas till en annan myndighet, om uppgiftsskyldighet följer av lag eller förordning.

Det finns inte något konstitutionellt hinder mot att regeringen medger att annars sekretessbelagda uppgifter lämnas mellan myndigheter eller självständiga verksamhetsgrenar inom en myndighet. I förarbetena till motsvarande bestämmelse i den tidigare sekretesslagen (1980:100) anfördes att det däremot från saklig synpunkt i vissa fall kan te sig tveksamt att regeringen kan tunna ut en av riksdagen i lag beslutad sekretess till skydd för enskilda genom föreskrifter som medger att information lämnas från en myndighet till en annan eller mellan självständiga verksamhetsgrenar inom en myndighet (a. prop. s. 322). Regeringen kan dock inte genom föreskrifter i en förordning sätta åt sidan bestämmelser i lag som exklusivt reglerar uppgiftsutbytet mellan myndigheter.

För att det ska vara fråga om uppgiftsskyldighet i den mening som avses i paragrafen krävs att bestämmelsen i fråga uppfyller vissa krav på konkretion. Den kan ta sikte på utlämnande av uppgifter av ett speciellt slag, gälla en viss myndighets rätt att få del av uppgifter i allmänhet eller avse en skyldighet för en viss myndighet att lämna andra myndigheter information (Lenberg m.fl., kommentaren till 10 kap. 28 §).

En föreskrift som mera generellt anbefaller samverkan mellan myndigheter är däremot inte av sådant slag att den kan anses ålägga en uppgiftsskyldighet i den mening som avses i paragrafen. Exempelvis är bestämmelserna i 6 kap. 5 § OSL och 6 § FL inte av det slaget.

Ytterligare sekretessbrytande bestämmelser som tar sikte på uppgiftsutbyte mellan myndigheter i vissa fall finns också i 10 kap. 15–26 §§ OSL, bl.a. för brottsbekämpande ändamål.

Överföring av sekretess

När en sekretessbelagd uppgift lämnas från en myndighet till en annan är huvudregeln att sekretessen inte följer med uppgiften. Det har emellertid införts bestämmelser om överföring av sekretess inom vissa områden.

Ett exempel på en bestämmelse om överföring av sekretess är 11 kap. 4 § OSL. Där föreskrivs i första stycket att om en myndighet har elektronisk tillgång till en upptagning för automatiserad behandling hos en annan myndighet och en uppgift i denna upptagning är sekretessreglerad, blir sekretessbestämmelsen tillämplig även hos den mottagande myndigheten. Enligt andra stycket ska första stycket inte tillämpas på en uppgift som ingår i ett beslut hos den mottagande myndigheten.

Bakgrunden till bestämmelsen i 11 kap. 4 § första stycket OSL är att en myndighet som medgetts direktåtkomst kan behöva få teknisk tillgång till fler uppgifter än de uppgifter som myndigheten behöver och därmed har rätt att behandla, s.k. överskottsinformation (prop. 2007/08:160 s. 75).

Av 11 kap. 8 § följer att 4 § inte ska tillämpas om det finns en s.k. primär sekretessbestämmelse som redan är tillämplig på uppgifterna hos den mottagande myndigheten. Vi har i vårt delbetänkande Överskottsinformation vid direktåtkomst (SOU 2012:90) föreslagit att det ska införas ett andra stycke i 11 kap. 8 §, där det föreskrivs att första stycket inte ska tillämpas på en uppgift som är tillgänglig för en myndighet på sätt som anges i 11 kap. 4 § första stycket och som den mottagande myndigheten enligt lag eller förordning inte får behandla.

5.2.3 Personuppgiftslagen

I personuppgiftslagen finns inga bestämmelser som direkt tar sikte på uppgiftsutbyte mellan myndigheter. Flera av bestämmelserna i lagen har dock betydelse för i vilken omfattning ett utbyte av personuppgifter mellan myndigheter är möjligt. Både bestämmelserna med grundläggande krav på personuppgiftsbehandling i 9 § och regler om vilka typer av behandlingar som är tillåtna i 10 § och 13–22 §§ påverkar möjligheterna till sådant utbyte. Dessa krav gäller dock inte enligt det allmänt gällande undantaget i 5 a § – den s.k.

missbruksregeln – som tar sikte på behandling i ostrukturerat material. Detta undantag har dock genom en inkonsekvent reglering i särskilda registerförfattningar kommit att gälla för vissa myndigheter men inte för andra.

5.3 Uppgiftsutbyte genom direktåtkomst

5.3.1 Begreppet direktåtkomst

Det finns ingen legaldefinition av begreppet direktåtkomst. I tidigare registerförfattningar användes begreppet terminalåtkomst. Exempelvis föreskrevs i 10 och 12 §§ i den numera upphävda skatteregisterlagen (1980:343) vilka myndigheter som skulle få ha terminalåtkomst till det centrala skatteregistret respektive ett regionalt skatteregister.

Sedan slutet av 1990-talet används i stället begreppet direktåtkomst, eftersom terminaler hade kommit att användas alltmer sällan och begreppet terminalåtkomst därför ansågs föråldrat (se t.ex. prop. 1997/98:97 s. 88). Med direktåtkomst avses vanligtvis att någon har direkt tillgång till någon annans register eller databas och på egen hand kan söka efter information, dock utan att kunna påverka innehållet i registret eller databasen (se bl.a. prop. 2009/10:85 s. 168). I begreppet ligger också att den som är personuppgiftsansvarig för registret eller databasen inte har någon kontroll över vilka uppgifter som mottagaren vid ett visst söktillfälle tar del av (prop. 2011/12:45 s. 133). Den myndighet som lämnar ut uppgifter genom direktåtkomst fattar således inte något beslut om utlämnande av de uppgifter som den som har direktåtkomst tar del av i varje enskilt fall.

I förarbetena till 11 kap. 4 § OSL, som alltså reglerar överföring av sekretess vid direktåtkomst, uttalade sig regeringen om hur direktåtkomst bör definieras (prop. 2007/08:160 s. 164). Med en sådan åtkomst avsågs enligt regeringen att en upptagning är tillgänglig hos den mottagande myndigheten på ett sådant sätt som avses i 2 kap. 3 § andra stycket första meningen TF, dvs. upptagningen ska vara tillgänglig med tekniska hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas, avlyssnas eller på annat sätt uppfattas.

Högsta förvaltningsdomstolen fann i rättsfallet HFD 2011 ref. 52 att det förhållandet att handlingar i en databas gjorts tekniskt tillgängliga för en annan myndighet för bl.a. statistikframställning innebar att handlingarna måste anses expedierade i den mening som avses i 2 kap. 7 § TF. Av rättsfallet framgår att det är själva tillgången till handlingarna som innebär att de anses expedierade till den andra myndigheten. Huruvida den myndigheten i något konkret fall faktiskt hade använt sig av tillgången har således inte någon betydelse för bedömningen av om handlingarna var att anse som expedierade.

Den i rättsfallet aktuella begäran om att få ta del av allmänna handlingar gällde uppgifter som förts in i databasen från en myndighet. Frågan var om uppgifterna ingick i allmänna handlingar hos den myndigheten. Högsta förvaltningsdomstolen hade inte anledning att uttala sig beträffande frågan om det också var en allmän handling hos den mottagande myndigheten. Av domstolens slutsats att handlingarna gjorts tillgängliga för den myndigheten på ett sådant sätt att de hade expedierats, följer emellertid att de därmed är att anse som förvarade hos den mottagande myndigheten i den mening som avses i 2 kap. 3 § andra stycket TF.

Den omständigheten att direktåtkomst till en viss mängd uppgifter innebär att de handlingar i vilka uppgifterna ingår anses expedierade till den mottagande myndigheten medför alltså i sin tur att handlingarna är att anse som förvarade, och därmed också som huvudregel som inkomna, hos den myndigheten i den mening som avses i 2 kap. 3 och 6 §§ TF. Handlingarna utgör genom direktåtkomsten således allmänna handlingar även hos den mottagande myndigheten. En direktåtkomst till sekretessreglerade uppgifter innebär vidare att det krävs en sekretessbrytande regel för att utlämnandet av uppgifterna inte ska innebära ett brott mot den sekretess som annars gäller.

5.3.2 Hur regleras en myndighets direktåtkomst till en annan myndighets informationssamlingar?

Vid vår genomgång av registerförfattningar har det kommit fram att utlämnande i form av direktåtkomst regleras på i huvudsak tre olika sätt. Ett sätt är att i författning beskriva några fall då direktåtkomst får medges. Ett exempel på detta förfaringssätt är den

direktåtkomst som får medges till Skatteverkets beskattningsdatabas. I 7–8 a §§ lagen (2001:181) om behandling av uppgifter i Skatteverkets beskattningsverksamhet regleras vilka myndigheter, eller självständiga verksamhetsgrenar inom Skatteverket, som får ha direktåtkomst till beskattningsdatabasen. Förutom att föreskriva vilka myndigheter som ”får ha” direktåtkomst, anges också vilka uppgifter som direktåtkomsten får omfatta. Det anges också att regeringen meddelar närmare föreskrifter om vilka uppgifter och handlingar direktåtkomsten får omfatta.

I förordningen (2001:588) om behandling av uppgifter i Skatteverkets beskattningsverksamhet finns i 4–8 §§ bestämmelser om när uppgiftsskyldighet finns i förhållande till uppräknade myndigheter. I 8 a § erinras vidare om att uppgiftsskyldighet föreskrivs också i vissa omnämnda författningar.

Ett annat sätt är att uttömmande reglera i vilka fall direktåtkomst får medges. Denna lagstiftningsteknik har använts exempelvis i fråga om socialförsäkringsdatabasen som innehåller personuppgifter i Försäkringskassans och Pensionsmyndighetens verksamhet. I 114 kap. 18–23 §§ SFB finns bestämmelser om direktåtkomst till socialförsäkringsdatabasen. Av 2 och 5 §§ framgår att socialförsäkringsdatabasen utgörs av den samling av uppgifter som med hjälp av automatiserad behandling används gemensamt för handläggning av förmåner m.m. som utförs av Försäkringskassan och Pensionsmyndigheten.

Enligt 18 § är direktåtkomst till socialförsäkringsdatabasen endast tillåten i den utsträckning som anges i lag eller förordning. I 19–23 §§ finns därefter bestämmelser om vissa myndigheter eller organ med myndighetsuppgifter som, förutom Försäkringskassan och Pensionsmyndigheten, får ha sådan direktåtkomst och att det gäller i den utsträckning det behövs för särskilt nämnda ärendeslag eller ändamål. Vad gäller ändamålen hänvisas till 8 § där s.k. sekundära ändamål räknas upp, dvs. som tar sikte på tillhandahållande av information som behövs i annan verksamhet än den som bedrivs av Försäkringskassan och Pensionsmyndigheten. I 3–4 §§ förordningen (2003:766) om behandling av personuppgifter i socialförsäkringens administration finns ytterligare föreskrifter om direktåtkomst. Bestämmelser om uppgiftsskyldighet på socialförsäkringsområdet som knyter an till bestämmelserna om direktåtkomst i 114 kap. SFB finns vidare i förordningen (1980:995) om skyldighet för

Försäkringskassan och Pensionsmyndigheten att lämna uppgifter till andra myndigheter, den s.k. uppgiftslämnarförordningen. Sådana bestämmelser finns också i vissa fall i författningar som gäller den myndighet som medgetts direktåtkomst till socialförsäkringsdatabasen.

Direktåtkomst kan också regleras på det sättet att författningen ger uttryck för när direktåtkomst inte får förekomma, dvs. i form av förbud mot direktåtkomst. Så är fallet med direktåtkomst till personuppgifter inom socialtjänsten. Enligt 11 § lagen (2001:454) om behandling av personuppgifter inom socialtjänsten bemyndigas regeringen att meddela föreskrifter om bl.a. direktåtkomst. I 24 § förordningen (2001:637) om behandling av personuppgifter inom socialtjänsten föreskrivs att Socialstyrelsen får i verksamhet som avses i lagen (2007:606) om utredningar avseende vissa dödsfall inte medge andra myndigheter eller enskilda direktåtkomst till personuppgifter. I övrigt saknas bestämmelser om direktåtkomst. I den nya lagen (2014:484) om en databas för övervakning av och tillsyn över finansmarknaderna finns bestämmelser som innebär att vissa myndigheter inte bara får, utan ska, medges direktåtkomst (6 och 7 §§). Att man reglerar direktåtkomsten på ett sådant sätt hör emellertid till undantagen.

Det finns också exempel på att en myndighet har gett en annan myndighet direktåtkomst utan att det särskilt har reglerats. Ett sådant exempel är att Transportstyrelsen, efter samråd med Datainspektionen, har gett bl.a. Luftfartsverket direktåtkomst till luftfartsregistret. Det finns ingen särskild registerförfattning som reglerar behandling av personuppgifter i det registret, utan i stället gäller personuppgiftslagen. Att registret ska föras framgår dock av 2 kap. 1 § luftfartslagen (2010:500).

5.4 Uppgiftsutbyte genom utlämnande på medium för automatiserad behandling

5.4.1 Begreppet

Begreppet utlämnande på medium för automatiserad behandling används i registerförfattningar utan att begreppet har getts någon legaldefinition. Uttrycket ”automatiserad behandling” finns i flera paragrafer i personuppgiftslagen, t.ex. 5 §. I den tidigare datalagen

(1973:289) användes begreppet automatisk databehandling. Vid personuppgiftslagens införande konstaterade Lagrådet att det begreppet var väl inarbetat, men att ett sådant uttryckssätt förde tanken till en behandling som sker automatiskt efter en viss händelse eller tidpunkt e.d. oavsett hur behandlingen utförs. I stället borde uttrycket ”automatiserad behandling” användas. Regeringen instämde i denna bedömning (prop. 1997/98:44 s. 38 f. och 240). Begreppet automatiserad behandling har sedan kommit att användas i de registerförfattningar som tillkommit efter personuppgiftslagens införande. Även i 2 kap. TF används begreppet automatiserad behandling, i t.ex. 3 och 13 §§ talas om ”upptagning för automatiserad behandling”. Skälet är att man velat ansluta till terminologin i registerförfattningarna (prop. 2001/02:70 s. 23).

Vad som avses med ett medium för automatiserad behandling som kan användas för utlämnande av information har varierat beroende på informationsteknikens utveckling. I äldre förarbeten talades det exempelvis om magnetband, skivminnen eller en handling med visuellt läsbar text, om texten var maskinläsbar och avsikten var att avläsning skulle ske maskinellt (prop. 1979/80:146 s. 48). I senare motivuttalanden anfördes att utlämnande kunde ske genom filöverföring, på diskett eller på annat sätt med hjälp av automatisk databehandling (prop. 1995/96:201 s. 31).

Med dagens teknik kan utlämnande av information ske exempelvis genom e-post, på ett usb-minne eller genom direkt överföring från ett datorsystem till ett annat via ett elektroniskt kommunikationsnät. Vid ett mer omfattande uppgiftsutbyte mellan myndigheter är det ofta den senare metoden som används.

I studiestödsdatalagen skiljer man på begreppen utlämnanden på medium för automatiserad behandling och utlämnanden via elektronisk kommunikation (se 13 §). Med medium för automatiserad behandling avses ett fysiskt medium såsom diskett, usb-minne eller cd-skiva, medan utlämnanden via elektronisk kommunikation tar sikte på exempelvis e-post, sms eller skriftlig dialog i realtid via internet (prop. 2008/09:96).

5.4.2 Hur regleras utlämnande på medium för automatiserad behandling?

Frågan om utlämnande på medium för automatiserad behandling har behandlats på olika sätt i registerförfattningarna. I vissa författningar har man uttryckligen reglerat när ett sådant utlämnande får ske. Ett sådant exempel är utlämnanden från socialförsäkringsdatabasen, som regleras i 114 kap. 24 § SFB. Enligt den bestämmelsen får personuppgifter i socialförsäkringsdatabasen som får lämnas ut till den registrerade lämnas ut till denne på medium för automatiserad behandling. I övrigt får personuppgifter ur databasen lämnas ut på sådant medium endast om det behövs för något av de ändamål som anges i 8 och 9 §§, dvs. för ett av de där uppräknade tillåtna ändamålen för att tillhandahålla information – s.k. sekundära ändamål. Ett annat exempel där lagstiftaren har valt att reglera i vilka fall utlämnande på medium för automatiserad behandling ska vara tillåtet är studiestödsdatalagen (2009:287). Enligt 10 § är elektroniskt utlämnande tillåtet bara i den utsträckning som anges i lag eller förordning. Som ytterligare förutsättningar gäller att bestämmelserna om tillåtna ändamål i 4 § följs. Detsamma gäller bestämmelserna om särskilda begränsningar, samtycke och sökbegrepp i 6–8 §§. Av 13 § följer emellertid att när personuppgifter får lämnas ut till någon genom direktåtkomst, får de också på något annat sätt lämnas ut elektroniskt till mottagaren. Vidare får personuppgifter även i andra fall lämnas ut på medium för automatiserad behandling eller via elektronisk kommunikation i enskilda fall.

I andra författningar saknas det regler om utlämnande på medium för automatiserad behandling. Av förarbetena framgår att man då ansett att en sådan reglering inte är nödvändig för att ett utlämnande ska kunna ske. Som exempel kan nämnas utlämnanden från beskattningsdatabasen. Enligt 2 kap. 6 § lagen om behandling av uppgifter i Skatteverkets beskattningsverksamhet får uppgifter i databasen lämnas ut till enskild på medium för automatiserad behandling endast om regeringen har meddelat föreskrifter om det. För sådant utlämnande till en myndighet saknas däremot regler. Ett annat exempel där det inte bedömts nödvändigt att särskilt reglera utlämnanden på medium för automatiserad behandling för att det ska vara tillåtet är patientdatalagen (2008:355). I lagen har i stället införts en bestämmelse, 5 kap. 6 §, som föreskriver att om en

personuppgift får lämnas ut, kan det ske på medium för automatiserad behandling. Det uppställda villkoret syftar på att uppgiften inte kan lämnas ut om utlämnandet inte är en tillåten behandling av personuppgifter eller sekretess hindrar utlämnandet (prop. 2007/08:126 s. 77 och 246 f.).

Ett fåtal författningar innehåller förbud mot utlämnanden på medium för automatiserad behandling. Ett sådant exempel är utlämnanden från passagerarregistret. Enligt 7 § lagen (2006:444) om passagerarregister är det förbjudet att lämna ut personuppgifter ur registret på medium för automatiserad behandling. Bakgrunden till bestämmelsen behandlas inte närmare i förarbetena (prop. 2005/06:129). Det konstateras emellertid att en myndighet som begär att få ut uppgifter ur registret med stöd av den s.k. generalklausulen i 10 kap. 27 § OSL således inte kan få uppgifterna utlämnande på medium för automatiserad behandling (a. prop. s. 79).

5.5 Den tekniska utvecklingen

5.5.1 Tidigare uttalanden om den tekniska utvecklingens betydelse för begreppens innebörd

I våra direktiv anförs att den tekniska utvecklingen har inneburit att det numera finns betydligt fler sätt att överföra uppgifter elektroniskt än tidigare och att nya åtkomstmetoder alltjämt tillkommer. Detta har medfört att det uppfattas som oklart hur begreppen direktåtkomst och utlämnande på medium för automatiserad behandling ska tillämpas på modernare metoder för informationsutbyte.

I prop. 2007/08:160 behandlades frågan om ett utökat elektroniskt informationsutbyte mellan Migrationsverket, Försäkringskassan, Skatteverket, Kronofogdemyndigheterna, Statens Pensionsverk, Centrala studiestödsnämnden, Arbetsförmedlingen, arbetslöshetskassorna och kommunernas socialnämnder. Regeringen drog här slutsatsen att utgångspunkten för det utökade elektroniska informationsutbytet bör vara att utlämnandet av uppgifter ska ske genom att direktåtkomst medges (a. prop. s. 56 f.). När det gällde utlämnande som inte sker genom direktåtkomst utan på medium för automatiserad behandling anförde regeringen att den teknik som i dag används för sådan elektronisk informationsöverföring nor-

malt innebär att data utbyts nattetid och att begärd information skickas från de interna registren till en brevlåda hos den myndighet som ska lämna ut uppgifterna (a. prop. s. 58). Regeringen påpekade att den fördröjning i uppgiftslämnandet som är inbyggd i tekniken innebär en teoretisk möjlighet för utlämnaren att kontrollera vilken information som ska lämnas ut. Sekretessprövningen sker dock i praktiken i samband med att förbindelsen upprättas. Någon ytterligare prövning av uppgifterna i samband med utlämnandet sker inte vid överföringar via telenätet, även om det på grund av fördröjningen i systemen är teoretiskt möjligt att göra en sådan prövning. Regeringen ansåg att den tekniska utvecklingen har lett till att skillnaderna mellan direktåtkomst och annat utlämnande på automatiserad väg har blivit så små att det kan vara svårt att dra en gräns mellan direktåtkomst och andra former för utlämnande.

I samma proposition påpekade regeringen vidare att s.k. batchkörningar, som ofta användes för utlämnande på medium för automatiserad behandling, har en tidsfördröjning på ett dygn (prop. 2007/08:160 s. 60). Detta innebär att de uppgifter som hämtats in från en annan myndighets system är i vart fall en dag gamla när handläggaren av ett ärende fattar beslut med stöd av dessa.

E-offentlighetskommittén påpekade i sitt betänkande Allmänna handlingar i elektronisk form – offentlighet och integritet (SOU 2010:4) att den tekniska utvecklingen har fört med sig att gränsen mellan de metoder för utlämnande i elektronisk form som förekommer i registerförfattningarna i viss mån har suddats ut (s. 366). Kommittén hänvisade i denna del till SAMSET-rapport 2006:1, Elektroniskt informationsutbyte – myndighetsgemensamma rättsfrågor, s. 78 ff.

Vi har i vårt delbetänkande berört frågan om vilka begrepp som används vid elektroniska utlämnandeformer och konstaterade där att begreppet utlämnande på medium för automatiserad behandling i takt med att tekniken utvecklats har getts en vidare innebörd än att avse ett överlämnande av elektroniskt lagrade uppgifter via något slags medium för lagring eller överföring (SOU 2012:90 s. 198 f.). Med hänvisning till uttalanden i förarbeten nämnde vi som exempel på detta s.k. batch-körningar.

E-delegationens expertgrupp för rättsliga frågor har i en rapport från mars 2012 presenterat en juridisk modell för on-lineliknande utlämnanden som syftar till att inte komma i konflikt med de krav i

författning som gäller för direktåtkomst, uppfylla erforderliga krav på persondataskydd och informationssäkerhet och inte leda till att överskottsinformation hos mottagande myndighet uppstår. Expertgruppen anför i rapporten att den snabba tekniska utvecklingen har möjliggjort att nya metoder för utlämnanden av myndighetsinformation kan innefatta reella och automatiserade kontroller som görs i varje enskilt fall, i likhet med vad som sker vid automatiserade beskattningsbeslut. Enligt expertgruppens bedömning kan ett fullt utvecklat stöd för automatiserade beslut, som leder till reella prövningar och individuella förvaltningsbeslut i varje enskilt fall innan uppgifter lämnas ut, ges en sådan utformning att informationsutbytet inte bör anses utgöra direktåtkomst.

5.5.2 Uppgiftsutbyte mellan Försäkringskassan och kommunala nämnder

För närvarande pågår en process i allmän förvaltningsdomstol mellan Försäkringskassan och Datainspektionen där frågan berörs om ett uppgiftsutbyte mellan Försäkringskassan och kommunala nämnder är att anse som direktåtkomst eller utlämnande på medium för automatiserad behandling. Uppgiftsutbytet sker genom datasystemet LEFI Online, som är en automatiserad onlinetjänst som bl.a. ger socialnämnder åtkomst till viss information. Det är en fråga/svarstjänst med fördefinierade frågor och svar. Mottagaren skickar en frågefil avseende en viss person i taget som innehåller uppgifter om personnummer och efterfrågade förmåner för en viss period. Försäkringskassans it-system hämtar in informationen från olika interna källor och sammanställer ett svar. En behörighetskontroll och två sekretesskontroller genomförs automatiserat under processen. En svarsfil skickas sedan till mottagaren.

I sak rör målet om Datainspektionen, som anser att det uppgiftsutbyte som sker genom LEFI-Online är direktåtkomst, haft fog för ett föreläggande mot Försäkringskassan att upphöra med att ge socialnämnder åtkomst till uppgifter i socialförsäkringsdatabasen till dess att en sådan försäkran som avses i 114 kap. 22 § SFB har hämtats in från socialnämnderna.

I en dom den 19 december 2012 (mål nr 9049-11) fann Förvaltningsrätten i Stockholm att det måste vara fråga om ett beslut som baseras på en reell prövning i det enskilda fallet för att det ska vara

fråga om utlämnande på medium för automatiserad behandling och inte direktåtkomst. Det bör enligt förvaltningsrätten krävas att en sådan prövning inte endast innebär i princip detsamma som en på förhand genomförd prövning vid direktåtkomst till fördefinierade uppgifter. Domstolen instämde därför i Datainspektionens bedömning att det var fråga om direktåtkomst och ansåg att det därmed saknades anledning att invända mot Datainspektionens föreläggande.

Försäkringskassan överklagade domen till Kammarrätten i Stockholm, som i en dom den 14 februari 2014 avslog överklagandet (mål nr 189-13). Som skäl för sitt avgörande anförde kammarrätten bl.a. följande. För att det ska vara fråga om ett utlämnande på medium för automatiserad behandling krävs antingen att det är fråga om en s.k. batch-körning eller att utlämnandet baseras på en reell prövning i det enskilda fallet. Med en reell prövning avses att den utlämnande myndigheten i varje enskilt fall gör en sekretessprövning av om uppgifter kan lämnas ut. I målet var det inte fråga om en batch-körning. Vad gällde frågan om en reell sekretessprövning görs vid utlämnande av uppgifterna, framgick av handlingarna i målet att Försäkringskassan inte fattar något individuellt beslut, automatiserat eller inte, för varje enskild begäran. Vid en sammantagen bedömning av de behörighets- och sekretesskontroller som utförs i systemet LEFI Online av de fördefinierade uppgifterna fann kammarrätten att de inte kan anses tillräckliga för att det ska anses som att det sker ett utlämnande på medium för automatiserad behandling, utan att utlämnandet som sker genom systemet sker genom direktåtkomst.

Försäkringskassan har överklagat kammarrättens dom till Högsta förvaltningsdomstolen som beslutade att meddela prövningstillstånd den 21 januari 2015 (mål nr 1356-14).

5.5.3 Självbetjäningstjänster

En del myndigheter har infört servicesystem som innebär att myndigheter och enskilda medges en automatiserad tillgång till uppgifter hos myndigheten som inte är sekretessreglerade, dvs. som inte omfattas av någon sekretessbestämmelse. Ett exempel är att man kan få tillgång till uppgifter i vägtrafikregistret genom själv-

betjäningstjänster via Transportstyrelsens hemsida. Möjligheten för Transportstyrelsen att medge direktåtkomst till registret är begränsad enligt särskilda bestämmelser i lagen (2001:558) om vägtrafikregister och den anknytande förordningen (2001:650). Transportstyrelsen har i en framställan till regeringen den 16 juni 2014 uppmärksammat att det nuvarande regelverket inte ger ett tydligt stöd för de redan befintliga servicetjänsterna och är ett hinder för fortsatt utveckling av dessa (dnr TSV 2014-1642). Myndigheten föreslår därför vissa ändringar i nämnda registerförfattningar, bl.a. att direktåtkomst till enstaka personuppgifter som gäller registrering av fordon, felparkeringsavgifter samt trängselskatt och som inte är integritetskänsliga ska vara tillåtna utan något särskilt medgivande och utan att ändamålen med åtkomsten behöver prövas.

Många myndigheter ger enskilda möjlighet att via en ”allmänhetens terminal” själva söka i myndighetens diarier och andra informationssamlingar med offentliga uppgifter som myndigheten gjort tillgängliga för sökning i terminalen. En sådan ”allmänhetens terminal” kan ses som ett praktiskt sätt att lösa den skyldighet för myndigheten som följer av 6 kap. 6 § OSL och som innebär att en myndighet som huvudregel ska ge enskilda tillfälle att själva använda tekniska hjälpmedel för att kunna ta del av myndighetens elektroniska handlingar. Detta sätt att erbjuda enskilda en teknisk möjlighet att direkt hos myndigheten ta del av elektroniska handlingar har ibland inte ansetts utgöra direktåtkomst (se t.ex. Ds 2013:10 s. 138). I andra sammanhang har ”allmänhetens terminal” emellertid betraktats som direktåtkomst (se t.ex. JK:s beslut den 20 januari 2010, dnr 7004-13-28).

5.6 Effektivitetsvinster och integritetsrisker

5.6.1 Uppdraget

I våra direktiv sägs att vi mot bakgrund av gränsdragningsproblematiken i fråga om direktåtkomst och utlämnande på medium för automatiserad behandling ska analysera vilka effektivitetsvinster och integritetsrisker som är förknippade med olika former av elektroniskt informationsutbyte.

5.6.2 Effektivitetsvinster

I syfte att effektivisera förvaltningen har riksdag och regering återkommande i olika lagstiftningsärenden infört bestämmelser som ska möjliggöra ett utökat elektroniskt informationsutbyte mellan olika myndigheter. En utgångspunkt har därvid ofta varit att det utökade elektroniska utbytet ska ske i form av direktåtkomst. I exempelvis prop. 2007/08:160 s. 56 f. om ett utökat elektroniskt informationsutbyte mellan Migrationsverket, Försäkringskassan, Skatteverket, Kronofogdemyndigheten, Statens pensionsverk, Centrala studiestödsnämnen, Arbetsförmedlingen, arbetslöshetskassorna och socialnämnder bedömdes att enbart den föreslagna elektroniska hanteringen av informationsutbytet mellan Försäkringskassan och Migrationsverket skulle frigöra ca 15 årsarbetskrafter från ett rutinbetonat uppgiftsinhämtande över telefon till mer kvalificerade arbetsuppgifter.

Riksrevisionen har i sin rapport RiR 2010:18 redovisat sin granskning av om möjligheterna till effektivisering har utnyttjats när det gäller informationsutbytet mellan myndigheter med ansvar för trygghetssystem. Enligt Riksrevisionens bedömning hade myndigheterna inte utnyttjat alla möjligheter som lag och teknik erbjuder. Ett införande av elektroniskt informationsutbyte mellan kommuner och myndigheter skulle kunna medföra en årlig nettobesparing på 150 miljoner kronor per år. Granskningen visade att det fortfarande fanns en stor utvecklingspotential i informationsutbytet mellan myndigheterna och att regeringens insatser på området inte hade nått ända fram. Enligt Riksrevisionen utgör den svåröverskådliga strukturen i lagstiftningen ett hinder för utbytet eftersom den skapar en osäkerhet hos myndigheterna om vilken information som får utbytas. De är vidare svårt att bedöma om det finns restriktioner i lagstiftningen när det gäller på vilket sätt det elektroniska utbytet får ske. Modellen med förvaltningsmyndigheter under regeringen och kommunalt självstyre innebar enligt Riksrevisionens bedömning att regeringen behövde bli bättre på att samordna resurser och att skapa ekonomiska incitament för myndigheterna. Elektroniskt informationsutbyte bör ske enligt gemensam standard så att säkerhet och därmed integritetsskyddet säkerställs i informationsöverföringen. En standardiserad kommunikationslösning bör bygga på modern och kostnadseffektiv teknik.

Riksrevisionen konstaterade vidare att det fanns exempel på att informationsutbyten inte har blivit av på grund av att myndigheterna hade problem med att tolka lagstiftningen om hur information får överföras, men att myndigheterna inte hade informerat regeringen om väsentliga problem med lagstiftning och resurser. En annan anledning till uteblivet informationsutbyte var kommunernas bristande samordning. Enligt Riksrevisionens uppfattning har myndigheterna ett gemensamt ansvar för att se till att viktiga informationsutbyten kommer till stånd samt att de bör skapa direktåtkomst för att effektivisera elektroniska utbyten i de fall det är ekonomiskt lönsamt. När det gällde problem i de elektroniska informationsutbyten som myndigheterna redan hade skapat visade granskningen att det förekom att informationen kunde utebli eller innehålla fel. Utbyte av information genom översändningar av batchfiler en gång per dygn medförde vidare en fördröjning av viktig information som behövs i handläggningen. Enligt Riksrevisionen borde sådana brister i det befintliga elektroniska informationsutbytet kunna åtgärdas genom en uppgradering av de tekniska systemen så att aktörerna får direktåtkomst till informationen.

I sin uppföljningsrapport år 2013 redovisade Riksrevisionen vilka åtgärder som vidtagits efter 2010 års granskning av informationsutbytet mellan myndigheter med ansvar för trygghetssystem. Riksrevisionen konstaterade bl.a. att regeringen i budgetpropositionen för år 2013 delade revisionens slutsats att myndigheternas handläggning kan effektiviseras, att regeringen under 2011 och 2012 tillsatt två utredningar med koppling till informationsutbytet (bl.a. Informationshanteringsutredningen), att E-delegationen i betänkandet Vägen till en effektivare e-förvaltning (SOU 2011:67) tagit fram en juridisk modell för en on-lineliknande åtkomst samt att Sveriges Kommuner och Landsting hade tagit fram ett strategidokument i syfte att stödja kommuner och landstings utveckling av e-förvaltning samt skapat ett programkontor med samordningsansvar.

I rapporten ESV 2014:2 redovisade Ekonomistyrningsverket sitt regeringsuppdrag att följa upp realiseringen av ekonomiska nyttor från e-förvaltningsprojekten Elektroniska fakturor, Elektroniska beställningar, Elektroniska legitimationer och Säker myndighetsgemensam meddelandeförmedling. Ekonomistyrningsverket redovisade i rapporten att det inte varit möjligt att sammanställa eko-

nomiska nyttor från de fyra initiativ som uppdraget omfattat. Den viktigaste orsaken var att initiativen fortfarande befann sig i en genomförandefas. Många myndigheter saknade vidare mätningar för genomförandet. Flera myndigheter hade också lyft fram att det saknades tillräckliga incitament för samverkan över myndighetsgränserna och för att mäta de ekonomiska nyttorna från dessa gemensamma satsningar.

På uppdrag av E-delegationen bedriver Centrala studiestödsnämnden projektet Effektiv informationsförsörjning. Projektets syfte är att ta fram en tjänst som möjliggör för kommuner att via en anslutning elektroniskt inhämta information från flera myndigheter samt Arbetslöshetskassornas samorganisation. Med den nya tjänsten kommer handläggaren att i stället för manuellt via brev, fax eller telefon kunna inhämta uppgifter från myndigheter och a-kassor på elektronisk väg. Tjänsten sattes i produktion i maj 2014 och bygger på Försäkringskassans befintliga it-tjänst LEFI-Online. Sveriges Kommuner och Landsting kommer att förvalta tjänsten. Utvecklingen sker i etapper och en pilotverksamhet startade våren 2014.

E-delegationen har utarbetat en vägledning för digital samverkan (uppdaterad senast i september 2014) som är ett första steg i att stödja organisationer som samverkar vid utveckling av gemensamma lösningar för informationssystem.

5.6.3 Integritetsrisker

Som vi har redovisat i vårt delbetänkande är det ett särskilt problem att s.k. överskottsinformation kan uppstå vid direktåtkomst. Detta beror på att när direktåtkomsten etableras det ofta inte går att avgöra exakt vilka specifika uppgifter i en värdmyndighets informationssamlingar som en mottagarmyndighet kan komma att ha anledning att ta del av. En sådan myndighet kan alltså behöva ha tillgång till uppgifter om personer som visar sig aldrig bli aktuella i myndighetens verksamhet. Detta kan redan i sig innebära vissa integritetsrisker. Det kan också få negativa konsekvenser för enskildas personliga integritet att överskottsinformation på detta sätt blir allmän handling hos mottagarmyndigheter redan då den tekniska möjligheten att ta del av informationen etableras.

En direktåtkomst kan också upplevas utgöra en risk för enskildas integritet i ett mer övergripande perspektiv, eftersom en sådan åtkomst aktualiserar särskilda frågor om informationssäkerhet på grund av att de inblandade aktörernas informationssystem i viss utsträckning kopplas samman.

Utlämnanden av personuppgifter i elektronisk form på annat sätt än genom direktåtkomst innebär däremot inte i sig att det uppstår vare sig problem med s.k. överskottsinformation eller sådana säkerhetsrisker som har samband med att informationssystemen kopplas samman. Däremot finns det integritetsrisker förknippade även med sådana former av informationsutbyte som bl.a. innebär att överväganden behöver göras så att information som behöver skyddas kan förmedlas på ett säkert sätt.

5.7 Våra överväganden

Bedömning: Direktåtkomst innebär rättsligt att gränsen mellan de uppgiftsutbytande myndigheterna i viss omfattning tas bort, vilket inte är en konsekvens av annat elektroniskt utlämnande. Hur den mottagande myndigheten väljer att använda direktåtkomsten har den utlämnande myndigheten inte någon befogenhet att påverka, eftersom de handlingar som omfattas av åtkomsten redan har lämnats ut. Korresponderande sekretessfrågor måste därför vara lösta på förhand liksom behov av sökbegränsningar hos den mottagande myndigheten, vilket kan medföra krav på lagstiftningsåtgärder. Både principiella och rättsliga skäl talar därför för att en åtskillnad mellan direktåtkomst och annat utlämnande i elektronisk form görs.

Vidare utgör varken den tekniska utvecklingen eller effektivitetsvinster och integritetsrisker som kan förknippas med olika åtkomstmetoder skäl för att utmönstra den begreppsmässiga åtskillnaden.

Ett sådant utlämnande i elektronisk form som inte är direktåtkomst innebär – oavsett på vilket sätt det sker – alltså inte att myndigheternas verksamhet rättsligt sett blandas samman. Något behov av att rättsligt skilja olika sådana former åt finns därför inte.

I våra direktiv sägs att vi ska ta ställning till om det finns skäl för att i registerförfattningar upprätthålla en skillnad mellan direktåtkomst och andra former av elektroniskt utlämnande eller om denna skillnad bör utmönstras. Vi uppfattar vårt uppdrag i denna del som att en analys bör göras av om det i lagstiftningssammanhang finns anledning att också i fortsättningen skilja på begreppen, dvs. att analysen bör ta sikte på begreppens rättsliga innebörd.

5.7.1 Att enbart beskriva direktåtkomst som en form av elektroniskt utlämnande ger en otillräcklig bild av vad åtkomsten rättsligt innebär

Visserligen kan direktåtkomst kort och gott beskrivas som en form av elektroniskt utlämnande. På detta sätt beskrivs begreppen också i flera förarbeten, exempelvis i motiven till studiestödsdatalagen (prop. 2008/09:96 s. 57 f.). Från en principiell och rättslig utgångspunkt ger den beskrivningen enligt vår mening emellertid en otillräcklig och alltför begränsad bild av vad en sådan åtkomst innebär. Termen direktåtkomst som sådan beskriver på ett bättre sätt vad det är frågan om, varvid nyckelordet är ”direkt”. Det tar sikte på att den utlämnande myndigheten bildligt talat öppnar sina dörrar för den mottagande myndigheten. Den mottagande myndigheten tillåts träda in innanför dörrarna och själv få, i den omfattning som medgetts, söka fritt i den utlämnande myndighetens informationssamlingar. Från ett principiellt perspektiv är den omständigheten att åtkomsten är direkt, dvs. att ”dörrarna öppnas”, det mest betydelsefulla, eftersom det innebär att den utlämnande myndigheten redan vid den tidpunkt då åtkomsten etableras har lämnat ut berörda uppgifter till den mottagande myndigheten. Denna omständighet gör att direktåtkomst är en betydligt mer vittomfattande form av elektroniskt utlämnande än andra sådana former av utlämnanden. Att direktåtkomsten är en speciell företeelse visas av att det uppstår både rättsliga och sakliga konsekvenser som inte uppkommer vid andra former av utlämnanden.

Konsekvenser såvitt avser allmänna handlingar och sekretess

En rättslig konsekvens är, som framgått ovan (avsnitt 5.3.1), att de upptagningar/handlingar hos den utlämnande myndigheten som direktåtkomsten omfattar blir expedierade i den mening som avses i 2 kap. 7 § TF redan i och med att åtkomsten etablerats, dvs. i den stund då upptagningarna är tekniskt tillgängliga för den mottagande myndigheten så att de kan läsas, avlyssnas eller på annat sätt uppfattas. Att en expediering sker innebär att handlingarna är att anse som allmänna både hos den utlämnande och mottagande myndigheten. Huruvida den mottagande myndigheten genom någon åtgärd faktiskt har använt sig av direktåtkomsten har ingen betydelse för denna fråga. Genom att åtkomsten etablerats är handlingarna alltså att anse som inkomna till och förvarade hos den mottagande myndigheten.

I och med att den mottagande myndigheten är insläppt och är ”innanför dörrarna” hos den utlämnande myndigheten kan den bland de uppgifter som direktåtkomsten omfattar själv välja om och i så fall vilka uppgifter den vill hämta hem till sina egna informationssamlingar genom någon form av faktiskt överföring för att därefter bearbeta uppgifterna där. Vad myndigheten väljer att göra har den utlämnande myndigheten inte någon rättslig befogenhet att påverka, eftersom handlingarna redan har lämnats ut till den mottagande myndigheten i 2 kap. TF:s mening genom att åtkomsten etablerats.

Till detta kommer att om man planerar att en direktåtkomst ska omfatta uppgifter hos en myndighet som är sekretessreglerade, är det nödvändigt att i förväg få klarlagt att åtkomsten är förenlig med den sekretess som gäller för respektive myndighets område. Dessa frågor måste alltså vara lösta innan direktåtkomsten etableras. För det första behöver det bedömas om det finns ett tillfredsställande sekretesskydd för uppgifterna hos den mottagande myndigheten eller om ett sådant skydd behöver införas. Det måste i så fall ske genom reglering i offentlighets- och sekretesslagen, dvs. genom lag. För det andra behöver det bedömas om det finns en sekretessbrytande regel som möjliggör att de sekretessreglerade uppgifterna lämnas ut till den mottagande myndigheten. Om inte, måste även en sådan föreskrift införas. Det kan ske i form av lag eller förordning. Eftersom en sekretessbrytande regel ska syfta till att göra direktåtkomsten möjlig måste en sådan regel ta sikte på direkt-

åtkomsten i dess hela vidd. Eftersom ett utlämnande sker av samtliga uppgifter som omfattas av direktåtkomsten i det ögonblick åtkomsten etableras, måste den sekretessbrytande regeln alltså möjliggöra hela detta utlämnande. Det är m.a.o. inte tillräckligt att en sekretessbrytande regel möjliggör ett utlämnande i de enskilda fall då den mottagande myndigheten genom en faktisk överföring använder sig av direktåtkomsten och hämtar vissa av de uppgifter som åtkomsten omfattar. Samtliga uppgifter har ju redan lämnats ut till den myndigheten i och med att direktåtkomsten har etablerats.

En rättslig konsekvens av en direktåtkomst är alltså att korrensponderande sekretessfrågor måste vara lösta i förväg, dvs. innan åtkomsten faktiskt etableras, vilket i sin tur i förekommande fall kan kräva författningsändringar.

I underlaget för bedömningen av vilken omfattning en sekretessbrytande regel ska ha, dvs. vilka uppgifter som ska lämnas ut genom direktåtkomsten utan hinder av sekretess, torde det i de flesta fall även behöva finnas med en analys av hur direktåtkomsten kan ordnas rent tekniskt. Först när en sådan analys är gjord torde man kunna ta ställning till hur omfattande direktåtkomsten behöver vara för att det planerade uppgiftsutbytet ska vara möjligt.

Konsekvenser såvitt avser behandling av personuppgifter och personuppgiftsansvar

Det finns också anledning att analysera vad en planerad direktåtkomst innebär i fråga om vilka behandlingar av personuppgifter som behöver ske samt när personuppgiftsansvaret aktualiseras och vad det tar sikte på. En direktåtkomst innebär att en rad förberedande åtgärder behöver vidtas som bl.a. inbegriper behandling av personuppgifter redan innan utlämnandet av uppgifterna sker. Det är en avgörande skillnad i förhållande till ett utlämnande av personuppgifter på automatiserat medium, som är begränsat till en behandling som innebär att uppgifter sänds över elektroniskt till mottagaren.

Vid en direktåtkomst behöver förberedande tekniska åtgärder vidtas för att direktåtkomsten, när den väl etableras, ska ta sikte på endast de personuppgifter som åtkomsten får omfatta. Det utgör en form av behandling av personuppgifter. Även andra förbered-

ande åtgärder behöver vidtas som har samband med inblandade myndigheters personuppgiftsansvar, även om de inte i sig innebär en behandling av personuppgifter. Det behöver exempelvis göras säkerhetsanalyser och krävs att eventuella behövliga åtgärder därefter vidtas för att motverka de risker för myndigheternas information som kan uppstå på grund av att deras tekniska system, och därmed verksamheter, i viss mån kopplas ihop genom direktåtkomsten. Andra förberedande åtgärder som den mottagande myndigheten behöver ägna sig åt i egenskap av personuppgiftsansvarig är att vidta tekniska och andra åtgärder, t.ex. fördelning av behörighet och åtkomstbegränsningar, för att säkerställa att endast de tjänstemän som har behörighet att använda sig av direktåtkomsten kommer att kunna göra det och att det kan kontrolleras och följas upp hur åtkomsten används. De inblandade myndigheterna har alltså ett gemensamt ansvar för att de säkerhets- och kontrollfrågor som direktåtkomsten ger upphov till är på ömse håll analyserade och lösta innan direktåtkomsten etableras. Frågor av dessa slag behandlas närmare i avsnitt 10.1.4 och 10.2.5.

När direktåtkomsten väl etableras sker också en behandling av personuppgifter, nämligen att samtliga uppgifter som omfattas av åtkomsten lämnas ut till den mottagande myndigheten genom att de vid etableringen blir tillgängliga för den myndigheten. Det är alltså något annat än den behandling av personuppgifter som sker när uppgifterna rent faktiskt förs över till den myndigheten. I den mån sådana faktiska överföringar sker är det behandlingar som utförs av den mottagande myndigheten när den använder sig av sin direktåtkomst. Det är också den myndigheten som enligt vad vi föreslår ska vara personuppgiftsansvarig för dessa behandlingar, se avsnitt 10.1.4. Detta är också en viktig skillnad i förhållande till hur ett s.k. utlämnande på automatiserat medium går till, då det är den utlämnande myndigheten som genomför och ansvarar för att personuppgifter faktiskt sänds över till den mottagande myndigheten.

En direktåtkomst som är igång innebär att de myndigheter som ingår i uppgiftsutbytet kommer att samtidigt utföra behandlingar av personuppgifter i den informationssamling som genom åtkomsten i viss mån blir gemensam. Både den utlämnande och mottagande myndigheten kommer alltså i olika delar och på olika nivåer att vara personuppgiftsansvariga för behandlingar som utförs. Den utlämnande myndigheten ansvarar exempelvis för innehållet i databasen

och för att kontrollera att det är rätt mottagande myndighet som använder direktåtkomsten. Den mottagande myndigheten i sin tur har t.ex. att svara för att det är en behörig handläggare som använder sig av åtkomsten för att hämta hem personuppgifter till de egna informationssamlingarna.

Frågor av detta slag kräver i allmänhet inte särskilt författningsstöd för att möjliggöra en direktåtkomst. Av 31 § PuL följer emellertid ett krav på den personuppgiftsansvarige att skydda de personuppgifter som ska behandlas genom åtgärder som ger en lämplig säkerhetsnivå. I samband med direktåtkomst måste alltså ställningstaganden och behövliga åtgärder av detta slag vidtas i förväg på myndighetsnivå. I den enskilde registrerades perspektiv är det vidare av stor vikt att det alltid ska vara tydligt vem som är personuppgiftsansvarig för en viss behandling. Den informationen ska vara lätt tillgänglig för den enskilde registrerade som alltid ska kunna veta vart man ska vända sig för att göra anspråk på sina rättigheter, exempelvis i form av rättelse eller skadestånd.

Konsekvenser såvitt avser användningen av sökbegrepp

Genom direktåtkomst blir den utlämnande myndighetens informationssamlingar i viss omfattning tillgängliga för den mottagande myndigheten på så sätt att den fritt kan söka och föra över uppgifter för att användas i den egna verksamheten. Dessa aktiviteter sker i den mottagande myndighetens verksamhet och omfattas således av de regler som gäller för den verksamheten och inte för den utlämnande myndighetens verksamhet. Det innebär vanligtvis att de eventuella sökbegränsningar som styr vilka sökningar och sammanställningar som kan göras i samband med den utlämnande myndighetens behandling av personuppgifter inte gäller för den mottagande myndigheten trots att denna genom direktåtkomsten får åtkomst till samma uppgifter. En fråga som därför också behöver analyseras i förväg innan en direkåtkomst medges är om det behövs regler som begränsar användningen av sökbegrepp för att uppnå ett tillfredsställande skydd för personuppgifter även hos den mottagande myndigheten. Det är ytterligare en rättslig konsekvens av direktåtkomst som inte uppstår i samband med ett utlämnande på medium för automatiserad behandling. I avsnitt 9.4 behandlar vi vilka sök-

begränsningar som generellt bör gälla vid myndigheters behandling av personuppgifter. Frågan om hur sökbegränsningar bör regleras vid direktåtkomst övervägs närmare i avsnitt 11.3.

Sammanfattning

I samband med direktåtkomst väcks alltså både principiella och rättsliga frågor som har sin grund i att gränsen mellan de uppgiftsutbytande myndigheterna i viss utsträckning tas bort. I förekommande fall krävs därför att ny sekretess respektive att en sekretessbrytande regel införs. En annan rättslig fråga är att det behöver övervägas om den mottagande myndighetens användning av de personuppgifter som blir åtkomliga genom direktåtkomst behöver begränsas genom förbud att använda vissa sökbegrepp. Inför etableringen av en direktåtkomst uppstår också ett behov av att inblandade myndigheter, i egenskap av verksamhets- och personuppgiftsansvariga, analyserar det tekniska genomförandet av åtkomsten samt vidtar förberedande åtgärder bl.a. för att åstadkomma en lämplig säkerhetsnivå på ömse håll. Samtliga dessa frågor, som alltså innebär att åtgärder behöver vidtas i vart fall på myndighetsnivå och eventuellt även av lagstiftaren, måste således vara lösta innan den mottagande myndigheten ”släpps in” hos den utlämnande myndigheten genom att direktåtkomsten etableras. Detta är en avgörande skillnad i förhållande till annat utlämnande som sker genom att uppgifter förmedlas i elektronisk form till mottagaren.

5.7.2 Annat utlämnande i elektronisk form ger inte i sig upphov till att särskilda åtgärder behöver vidtas

Vid utlämnanden i elektronisk form som inte sker genom direktåtkomst är det hela tiden den utlämnande myndigheten som rättsligt förfogar över frågan om och i så fall vilka uppgifter som ska lämnas ut genom att sändas över till den mottagande myndigheten. På detta sätt skiljer sig sådana utlämnanden i principiell mening från direktåtkomst. Bildligt talat kan det sägas innebära att den utlämnande myndigheten inte släpper in den mottagande myndigheten. Den mottagande myndigheten får i stället vänta ”utanför dörrarna” tills begärda uppgifter lämnas ut.

Konsekvenser såvitt avser allmänna handlingar och sekretess

I och med att den mottagande myndigheten inte släpps in till den utlämnande myndigheten uppstår inget behov av att analysera och eventuellt införa nya sekretessbestämmelser på grund av att gränsen mellan myndigheterna öppnas upp. Utlämnandet är alltså inte av ett sådant ingripande slag att det i sig, såsom vid direktåtkomst, medför ett behov av att i förväg analysera om författningsändringar behövs. Ett utlämnande sker i stället efter att den utlämnande myndigheten gjort en bedömning med utgångspunkt i de bestämmelser som är tillämpliga i det enskilda fallet. En helt annan sak är att det måhända kan finnas sekretessbestämmelser som kan tyckas i en oönskad utsträckning hindra ett visst uppgiftsutbyte mellan myndigheter.

Vid ett uppgiftsutbyte mellan två myndigheter som avses ha en någorlunda stor omfattning väcks den mer grundläggande frågan om det behövs regler för att styra huruvida sekretessreglerade uppgifter rutinmässigt kan lämnas ut till en annan myndighet. Den frågan bör övervägas skild från frågan om på vilket sätt uppgifter kan lämnas ut. Frågorna har emellertid ett samband på det sättet att om det finns behov av ett rutinmässigt uppgiftsutbyte, torde det utbytet kunna effektiviseras genom att utlämnandet sker i elektronisk form.

Ett rutinmässigt utlämnande av uppgifter till en annan myndighet kan regleras på så sätt att det införs en särskild sekretessbrytande regel för de myndigheter som ska utbyta information. Om så inte sker kan ett rutinmässigt utlämnande i stället äga rum med stöd av den s.k. generalklausulen i 10 kap. 27 § OSL, dvs. efter en avvägning mellan intresset av att skydda uppgifterna hos den utlämnande myndigheten och intresset hos den mottagande myndigheten av att få ut uppgifterna. Det kräver i sig alltså ingen särskild författningsreglering. Bestämmelserna i 10 kap. 27 § OSL bygger emellertid på att ett rutinmässigt utlämnande av sekretessreglerade uppgifter ska vara författningsreglerat (se avsnitt 5.2.2). Har det i en lag eller författning föreskrivits att uppgifter ”bör” eller ”får” lämnas ut får det antas att lagstiftaren har bedömt att intresset av att uppgifter lämnas mellan myndigheter har företräde framför sekretessintresset. Även om det inte är frågan om en sådan absolut uppgiftsskyldighet som avses i 10 kap. 28 § OSL, torde det

finnas ett relativt begränsat utrymme för den utlämnande myndigheten att i en konkret utlämnandesituation göra en annan bedömning. I rättslig mening är det dock den utlämnande myndigheten som förfogar över och beslutar om uppgifterna faktiskt ska lämnas ut. Även vid ett rutinmässigt utlämnande som får stöd i en författningsbestämmelse som föreskriver att uppgifter ”får” lämnas ut, är det alltså den utlämnande myndigheten som hela tiden rättsligt förfogar över frågan om uppgifterna ska lämnas ut.

I den händelse avsikten är att ett rutinmässigt uppgiftsutbyte ska äga rum mellan myndigheter och detta avser sekretessreglerade uppgifter, bör således utgångspunkten vara att uppgiftsutbytet bör komma till uttryck genom föreskrifter i lag eller förordning där det uttrycks att en myndighet ”bör” eller ”får” lämna ut uppgifter till en annan myndighet. Ett sådant behov av en författningsreglering har emellertid, som redan påpekats, inte något egentligt samband med frågan om på vilket sätt utlämnandet avses ske.

Konsekvenser såvitt avser behandling av personuppgifter och personuppgiftsansvar

Ett utlämnande i elektronisk form, som inte sker genom direktåtkomst utan genom att uppgifter elektroniskt sänds över till den mottagande myndigheten, medför inte samma krav på att förberedande analyser och åtgärder vidtas. Det enda som ska ske rent tekniskt är att uppgifterna i någon form sänds över från den utlämnande till den mottagande myndigheten. Några förberedande behandlingar av personuppgifter behöver alltså inte ske. Det är också endast översändandet som behöver analyseras från säkerhetssynpunkt och det resultatet kan styra i vilken form översändandet bör ske för att inga säkerhetsrisker ska uppstå för vare sig uppgifterna eller myndigheten. Det kan exempelvis innebära att uppgifter som avses sändas över via e-post bör krypteras.

Den utlämnande och den mottagande myndigheten behandlar inte heller vid något tillfälle de aktuella personuppgifterna samtidigt såsom är fallet vid direktåtkomst. Det uppstår alltså inte heller några frågor om hur personuppgiftsansvaret ska eller bör fördelas vid sådan samtidig behandling.

Konsekvenser såvitt avser användningen av sökbegrepp

Som redan påpekats är ett annat utlämnande i elektronisk form än genom direktåtkomst endast att se som en fråga om på vilket sätt uppgifter ska sändas över från en myndighet till en annan. I sig påkallar alltså inte utlämnandet några överväganden om vilka sökbegrepp den mottagande myndigheten ska få använda då den behandlar de uppgifter som hämtas in.

Sammanfattning

De frågor som väcks i samband med ett utlämnande i elektronisk form, som inte sker genom direktåtkomst, är väsentligen av annat slag och påkallar normalt sett inte åtgärder från lagstiftaren i det enskilda fallet. De frågor som uppstår begränsar sig till vad som har samband med det som saken rent faktiskt rör, nämligen att på ett eller annat sätt förmedla eller vidaresända personuppgifter elektroniskt. Några förberedande analyser och åtgärder behöver alltså inte vidtas annat än för att den utlämnande myndigheten ska kunna försäkra sig om att översändandet sker på ett säkert sätt. De rättsliga frågor som uppstår är vidare av ett mer allmänt slag. Det kan exempelvis röra förvaltningsrättsliga frågor om vem som är behörig att på myndighetens vägnar fatta beslut om utlämnande, motivering av beslut om en begäran helt eller delvis inte bifalls och möjlighet för den myndighet som nekas att få ut uppgifter att överklaga (jfr 6 kap. 7 § andra stycket OSL).

5.7.3 Vilken betydelse har den tekniska utvecklingen?

Av 8 kap. 1 § OSL följer att sekretess gäller även mellan myndigheter. Vidare framgår av 2 § att detsamma gäller också mellan olika verksamhetsgrenar inom en myndighet när de är att betrakta som självständiga i förhållande till varandra. Dessa bestämmelser innebär att det finns gränser myndigheterna emellan, och vissa fall också inom myndigheterna, som begränsar deras möjligheter att fritt utbyta sekretessreglerade uppgifter. Att motsvarande gränser i princip gäller även vid överlämnande av handlingar mellan och inom myndigheter på så sätt att ett överlämnande över myndighetsgräns-

erna innebär att handlingarna anses inkomna och upprättade och därmed som allmänna framgår av 2 kap. 8 § TF.

I rättsfallet HFD 2011 ref. 52 kom alltså Högsta förvaltningsdomstolen fram till att en myndighets tillgång till en annan myndighets databas på så sätt att den förstnämnda myndigheten där kunde ta del av uppgifter ”i läsbart skick” innebar att uppgifterna skulle anses expedierade i den mening som avses i 2 kap. 7 § TF och därmed utgöra en upprättad allmän handling. Den omständigheten att den mottagande myndigheten har getts en tillgång som innebär att den kunde läsa uppgifter i databasen innebär i sin tur att handlingar hade överlämnats till den myndigheten och därmed finns i dess förvar. Högsta förvaltningsdomstolen använder inte begreppet direktåtkomst, men kan anses indirekt konstatera att en direktåtkomst är för handen när det finns en sådan teknisk tillgång som avses i 2 kap. 3 § andra stycket TF. Domstolen får därmed uppfattas ha bekräftat den definition av direktåtkomst som getts i förarbetena till 11 kap. 4 § OSL, som reglerar överföring av sekretess vid direktåtkomst. Där anförde regeringen (prop. 2007/08:160 s. 164) att med sådan åtkomst avses att en upptagning är tillgänglig hos den mottagande myndigheten på ett sådant sätt som avses i 2 kap. 3 § andra stycket första meningen TF, dvs. upptagningen ska vara tillgänglig med tekniska hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas, avlyssnas eller på annat sätt uppfattas. Rättsfallet kan också sägas bekräfta det som enligt andra förarbetsuttalanden anses kännetecknа en direktåtkomst, nämligen att den mottagande myndigheten har en direkt tillgång till någon annans register eller databas och på egen hand kan söka information och att den utlämnande myndigheten inte har någon kontroll över vad mottagaren vid ett visst söktillfälle tar del av (se t.ex. prop. 2011/12:45 s. 133). Båda dessa omständigheter kan sägas vara ett resultat av att de upptagningar som omfattas av direktåtkomsten finns i den mottagande myndighetens förvar i den stund åtkomsten etableras.

De uttalanden som gjorts i förarbetena till 11 kap. 4 § OSL, vilka som vi ser det får anses ha bekräftats i rättsfallet HFD 2011 ref. 52, kan således sägas ge en definition av direktåtkomst, dvs. att en sådan åtkomst är för handen när den mottagande myndigheten har en sådan teknisk tillgång till den utlämnande myndighetens upptagningar som avses i 2 kap. 3 § andra stycket TF.

Rättspraxis ger däremot inte något omedelbart svar på hur man bör se på sådana former av elektroniskt utlämnande som ansetts befinna sig i en ”gråzon” mellan direktåtkomst och annat elektroniskt utlämnande, exempelvis s.k. batch-körningar och olika former av fråga/svar-tjänster. De nämnda företeelserna kan sägas vara kännetecknade av att den mottagande myndigheten har getts en möjlighet att tekniskt ansluta sig till den utlämnande myndighetens informationssamlingar, men möjligheten att genom en faktisk överföring hämta hem uppgifter är i någon mening inte direkt. Exempelvis sker ett utlämnande av begärda uppgifter först efter en viss tidsfördröjning eller efter att vissa automatiserade kontroller gjorts. Denna typ av omständigheter har ibland ansetts tala för att det inte är frågan om direktåtkomst utan om annat elektroniskt utlämnande, även om det är fråga om helt automatiserade system för utbyte av uppgifter mellan myndigheter. I den mån så skulle vara fallet, är det alltså endast den mängd uppgifter som överförs i de enskilda fallen som anses utlämnade till och därmed utgör allmänna handlingar hos den mottagande myndigheten. Att den mottagande myndigheten tekniskt sett har ”kopplat upp sig” mot den andra myndighetens uppgiftssamlingar och därigenom getts möjlighet att genom ett tekniskt förfarande begära ut uppgifter skulle vid ett sådant synsätt inte i sig anses innebära något utlämnande av uppgifter i tryckfrihetsförordningens mening.

Det är alltså inte givet i vilken utsträckning detta slags omständigheter har betydelse för frågan om den mottagande myndigheten har en sådan teknisk tillgång till uppgifter som avses i 2 kap. 3 § andra stycket TF, dvs. vad de betyder för frågan om en upptagning är att anse som förvarad hos den mottagande myndigheten genom att den kan läsas, avlyssnas eller på annat sätt uppfattas. Med andra ord står det inte helt klart vilka krav som formuleringen ”läsas, avlyssnas eller på annat sätt uppfattas” innefattar för att en teknisk åtkomst ska anses ”direkt”.

Den tekniska utvecklingen har även inneburit att myndigheterna har utvecklat tjänster som ger enskilda möjligheter att genom ett automatiserat förfarande ta del av myndigheternas informationssamlingar. Som exempel kan nämnas s.k. självbetjäningstjänster via myndigheternas hemsidor. Sådana former av tillgång till myndigheters uppgifter har ibland inte betecknats som direktåtkomst, trots att det i praktiken knappast kan vara frågan om något annat. En

möjlig förklaring kan vara att det då är fråga om offentliga uppgifter medan begreppet direktåtkomst har tenderat att förbehållas de fall där en automatiserad åtkomst kan anses särskilt känslig, t.ex. om en åtkomst tar sikte på sekretessreglerade uppgifter eller av annat skäl anses känslig från integritetsskyddssynpunkt.

Både den rättsliga och den tekniska utvecklingen kan således eventuellt komma att innebära att begreppet direktåtkomst inte kan göras liktydigt med automatiserat uppgiftsutlämnande, utan att begreppet bör ges en snävare innebörd. Oavsett hur denna fråga kan komma att besvaras i praxis kan det konstateras att det ändå kommer att finnas former av uppgiftsutbyte som tveklöst är att betrakta som direktåtkomst. I fråga om sådant uppgiftsutbyte finns det alltså anledning att också i fortsättningen principiellt och rättsligt skilja direktåtkomst från andra former av elektroniskt utlämnande. Det finns också i fortsättningen behov av att skilja på den ingripande form av utlämnande som en direktåtkomst innebär, som principiellt och rättsligt innebär att gränsen mellan de inblandade myndigheterna i viss mån försvinner, från andra elektroniska utlämnanden som inte har samma ingripande rättsliga konsekvenser och som inte i sig medför att det uppstår rättsliga frågor som måste lösas på förhand. Den tekniska utvecklingen utgör alltså i sig inget skäl för att utmönstra begreppet direktåtkomst.

5.7.4 Effektivitetsvinster och integritetsrisker

I flera lagstiftningsärenden som syftat till att utöka informationsutbytet mellan myndigheter har framhållits att utbytet kan effektiviseras om utbytet sker elektroniskt och i synnerhet om det sker genom direktåtkomst. Även Riksrevisionen bedömde i sin granskningsrapport från år 2010 (RiR 2010: 18) om informationsutbytet mellan myndigheter med ansvar för trygghetssystem att direktåtkomst medförde en större effektivisering än det elektroniska informationsutbyte som vid denna tid redan ägde rum i andra former.

Arbetet med att effektivisera myndigheternas verksamhet genom elektroniskt informationsutbyte har fortskridit och pågår alltjämt, bl.a. genom E-delegationens arbete. Under senare år har nya tekniska former för sådant utbyte tagits fram som, oavsett om det är

fråga om direktåtkomst eller inte, innebär effektiviseringar i förhållande till hur utbytet tidigare ägde rum.

Mot bakgrund av de utredningar som har gjorts i fråga om hur myndigheternas informationsutbyte kan effektiviseras och om ekonomiska nyttoeffekter av sådana projekt synes frågan om hur den bästa effektiviteten kan uppnås för närvarande inte handla så mycket om vilken elektronisk utlämnandeform som bör väljas utan mer om myndigheternas möjlighet att över huvud taget åstadkomma det informationsutbyte som regeringen eller de själva vill ska ske. Problem med att åstadkomma en önskad effektivisering förefaller till viss del handla om legala förutsättningar för ett visst informationsutbyte, men det kan också handla om brist på resurser i fråga om medel och kompetens samt att nödvändig samverkan inte kan åstadkommas.

En vanlig utgångspunkt är att direktåtkomst antas vara det mest effektiva sättet att utbyta information. Huruvida det också är det mest kostnadseffektiva sättet att utbyta information kan emellertid endast bedömas utifrån omständigheterna i det enskilda fallet. I fråga om ett visst informationsutbyte kan alltså andra former av elektroniskt informationsutbyte än direktåtkomst vara det mest effektiva. Vilken form av elektroniskt informationsutbyte som är mest effektiv, inbegripet ett kostnadsperspektiv, behöver alltså bedömas utifrån vilket konkret informationsutbyte det handlar om och i vilka former detta sker. Av betydelse är vidare vilken förmåga inblandade myndigheter har att åstadkomma det som faktiskt önskas av dem, det gäller inte minst i form av medel och resurser i övrigt. Till detta kommer att, även i de fall lagstiftaren väljer att i författning reglera ett visst informationsutbyte, det i slutändan regelmässigt står den enskilda myndigheten fritt att bestämma vilken utlämnandeform som ska väljas inom ramen för befintliga legala och andra förutsättningar.

Enligt vår bedömning går det inte att generellt uttala sig om vilken form av elektroniskt informationsutbyte som är det mest effektiva. Vi ser alltså ingen anledning att från ren effektivitetssynpunkt förorda någon viss metod.

De särskilda integritetsrisker som anses förknippade med direktåtkomst har samband med vilka tekniska åtgärder som vidtas för att så långt som möjligt minimera s.k. överskottsinformation, att överväga behovet av sekretesskydd i tillräcklig utsträckning och att

överväga vilka sökbegränsningar som bör gälla hos den myndighet som tar emot information genom sådan åtkomst. Vi redovisar i avsnitt 11.1 och 11.3 våra överväganden om hur sådana frågor bör regleras. I avsnitt 11.2 finns våra överväganden i frågan om andra elektroniska utlämnanden behöver en särskild reglering för att ge personuppgifter ett tillfredsställande skydd.

Sammanfattningsvis bedömer vi att det kan finnas effektivitetsvinster och integritetsrisker med alla former av elektroniskt utlämnande. Vilka vinster eller risker som uppstår hör emellertid inte så mycket samman med vilken form som väljs, utan vilket konkret informationsutbyte det är frågan om samt vilka förutsättningar det finns för aktuella myndigheter att över huvud taget välja utlämnandeform och att åstadkomma det informationsutbyte som tillgodoser krav på både effektivitet, även ur ett kostnadsperspektiv, och integritetsskydd. Varken effektivitetsvinster eller integritetsrisker utgör således skäl för att utmönstra en åtskillnad mellan olika elektroniska utlämnandeformer eller att förorda att ett elektroniskt informationsutbyte generellt bör ske i en viss form.

5.7.5 Principiella och rättsliga skäl samt krav på förberedande analyser och åtgärder medför behov av en fortsatt åtskillnad

En utgångspunkt för utredningens samtliga överväganden i de rättsliga frågor som ingår i uppdraget är bl.a. att så långt som möjligt underlätta en mer effektiv förvaltning, dvs. att så långt det är möjligt och lämpligt undanröja onödiga legala hinder.

Behovet av att rättsligt upprätthålla gränserna mellan myndigheter

Som har framgått är det med hänsyn till bestämmelserna i 2 kap. TF och offentlighets- och sekretesslagen av stor betydelse att det klargörs att direktåtkomst har omedelbara konsekvenser för frågor som rör myndigheternas gränser, vilken myndighet som förfogar över vilka uppgifter och problemet med överskottsinformation. Samma frågeställningar har också stor betydelse från en rent förvaltningsrättslig utgångspunkt. Det är bl.a. av vikt att det alltid står klart vad som hör till den verksamhet som en viss myndighet

ansvarar för. Att myndigheternas gränser i rättslig mening upprätthålls är således ett starkt rättssäkerhetskrav. Det kravet ställer i sin tur krav på inblandade myndigheter att på ömse håll agera i förväg och vidta nödvändiga åtgärder innan en direktåtkomst faktiskt medges, bl.a. för att säkerställa att en sådan åtkomst är förenlig med bestämmelser om sekretess.

Direktåtkomst medför krav på förberedande åtgärder ur verksamhets- och personuppgiftsansvarsperspektiv

Direktåtkomst innebär att viss behandling av personuppgifter behöver ske inför den faktiska etableringen och att inblandade myndigheter analyserar och löser de särskilda säkerhets- och kontrollfrågor som direktåtkomst från ett dataskyddsperspektiv ger upphov till. Även myndighetens personuppgiftsansvar innebär således att det ställs krav på att inblandade myndigheter gör klart för sig vilka åtgärder som behöver vidtas på ömse håll och hur ansvaret fördelar sig mellan dem. Detta utgör också skäl för att behålla en åtskillnad mellan direktåtkomst och annat elektroniskt utlämnande. Hur ett ansvar för skydd av personuppgifter ska fördelas mellan inblandade myndigheter vad gäller de olika åtgärder som behöver vidtas inom ramen för en direktåtkomst är emellertid inte givet. Denna fråga behandlas dock inte vidare här. Vi återkommer till den i kapitel 10.

Varken den tekniska utvecklingen eller effektivitetsvinster eller integritetsrisker utgör skäl för att utmönstra begreppet direktåtkomst

Som framgått anser vi att inte heller att den tekniska utvecklingen som sådan innebär att det finns skäl för att utmönstra begreppet direktåtkomst för att i stället generellt tala om elektroniskt utlämnande.

Inte heller de effektivitetsvinster eller integritetsrisker som kan uppstå vid olika former av elektroniska utlämnanden utgör skäl för att utmönstra begreppet direktåtkomst.

Direktåtkomst brukar beskrivas som en särskilt känslig form av uppgiftsutbyte, eftersom den anses innebära större risker för den enskildes integritet än då uppgifter lämnas ut efter en bedömning i

enskilda fall. Vi menar dock att en väl analyserad och förberedd direktåtkomst där man övervägt och löst frågor som rör sekretesskydd på ömse håll, vidtagit behövliga säkerhetsåtgärder, begränsat överskottsinformationen samt övervägt frågan om eventuella begränsningar i den mottagande myndighetens möjlighet att använda sig av de uppgifter som blir åtkomliga, inte behöver innebära större risker för den enskildes integritet än ett annat elektroniskt utlämnande av personuppgifter.

Vad som däremot kan innebära risker för den enskildes integritet i samband med direktåtkomst är att man inte beaktar de särskilda frågor och krav på skydd som den ger upphov till samt att man inte ägnar uppmärksamhet åt frågor som sammanhänger med att myndigheternas gränser öppnas upp och att därmed inblandade myndigheters ansvar för både verksamhet, säkerhet och personuppgifter behöver klargöras. Om man inte behåller en åtskillnad mellan begreppen direktåtkomst och annat elektroniskt utlämnande finns det enligt vår mening en risk för att dessa frågor inte får den uppmärksamhet som behövs för att på ett tillfredsställande sätt skydda den enskildes integritet.

Annat elektroniskt utlämnande än direktåtkomst medför inte behov av att klargöra myndigheters förhållande till varandra

Enligt vår uppfattning är det alltså den rättsliga skiljelinjen mellan direktåtkomst och annat elektroniskt utlämnande som är betydelsefull att behålla, eftersom den tydliggör vikten av att det ska stå klart i vilket förhållande de myndigheter som ingår i ett visst uppgiftsutbyte står till varandra. Utan den distinktionen riskerar myndigheternas respektive ansvar i olika hänseenden att bli otydligt. När det gäller olika former av andra elektroniska utlämnanden, dvs. vad som i dag betecknas som utlämnanden på medium för automatiserad behandling och som innebär att uppgifter i någon form sänds över eller förmedlas elektroniskt, uppstår inte samma behov av att klargöra frågor av det slaget. Ett sådant utlämnande innebär ju inte att myndigheternas verksamhet blandas samman rättsligt sett, oavsett på vilket sätt uppgifterna distribueras. De skillnader beträffande säkerhetsrisker som olika sätt att sända över uppgifter elektroniskt kan innebära utgör enligt vår mening inte något skäl till att göra någon rättslig åtskillnad mellan dem.

Vår bedömning är alltså att det från både principiella och rättsliga synpunkter finns starkt vägande skäl för att behålla en begreppsmässig skillnad mellan å ena sidan direktåtkomst och å andra sidan annat utlämnande i elektronisk form. Både principiella och rättsliga skäl samt konkreta krav på förberedande analyser och åtgärder talar med styrka för detta.

Som framgått har vi redan ovan redovisat en viss uppfattning för hur begreppet direktåtkomst bör avgränsas i förhållande till annat elektroniskt utlämnande. Vi återkommer i avsnitt 11.1 och 11.2 till hur begreppet direktåtkomst bör definieras och hur en generell reglering på myndighetsområdet rörande elektroniskt utlämnande bör se ut.

6 Behöver 6 kap. 5 § offentlighets- och sekretesslagen justeras för att undvika konflikt med internationella åtaganden?

6.1 Bakgrund

6.1.1 Uppdraget

Internationella avtal och sektorsspecifika rättsakter innehåller ibland artiklar om att en myndighet bara får använda uppgifter som erhålls enligt avtalet respektive rättsakten för vissa angivna ändamål eller i viss verksamhet. Sådana bestämmelser kan avse även andra uppgifter än personuppgifter. I Sverige anses en sådan bestämmelse inte utgöra ett hinder mot utlämnande av uppgifter med stöd av offentlighetsprincipen. Däremot kan en sådan användningsbegränsning anses stå i konflikt med en myndighets skyldighet att överlämna uppgifter till andra myndigheter enligt 6 kap. 5 § OSL. I våra direktiv framhåller regeringen att någon generellt tillämplig eller konsekvent genomförd lösning på sistnämnda typ av regelkonflikt saknas i lagstiftningen. I 9 kap. 2 § OSL ges visserligen en upplysning om att användningsbegränsningar införts i vissa andra författningar. Uppräkningen är emellertid inte heltäckande och det finns inte någon formell koppling mellan den bestämmelsen och 6 kap. 5 § OSL (jfr prop. 1990/91:131 s. 25). De författningar som avses i 9 kap. 2 § OSL utgör visserligen inte registerförfattningar. Enligt regeringen har den beskrivna frågeställningen dock en sådan betydelse för uppgiftsutbytet mellan myndigheter att den ändå bör utredas i detta sammanhang.

Vi har därför fått i uppgift att överväga om 6 kap. 5 § OSL bör justeras så att den står i bättre överensstämmelse med förekomsten

av nu nämnda användningsbegränsningar. Om vi finner att en sådan justering bör ske, ska författningsförslag lämnas.

6.1.2 Nuvarande bestämmelser

Informationsskyldigheten enligt 6 kap. 5 § OSL

Enligt 6 kap. 5 § OSL ska en myndighet på begäran av en annan myndighet lämna uppgift som den förfogar över, om inte uppgiften är sekretessbelagd eller det skulle hindra arbetets behöriga gång.

Bestämmelsen har redan behandlats i avsnitt 5.2, bl.a. vad avser förhållandet mellan informationsskyldigheten enligt paragrafen och föreskrifter om uppgiftsutlämnande enligt bl.a. 10 kap. 16–27 §§ OSL.

Informationsskyldigheten enligt 6 kap. 5 § OSL gäller för en uppgift som inte är sekretessbelagd, dvs. en uppgift för vilken sekretess inte gäller i den aktuella situationen. En myndighet kan alltså vara skyldig att lämna en uppgift till en annan myndighet som begär att få den om uppgiften inte alls är sekretessreglerad, dvs. om det inte finns någon bestämmelse om sekretess som är tillämplig på uppgiften. En skyldighet att lämna ut uppgiften finns också om den i och för sig är sekretessreglerad, men det inte innebär någon skada eller något men att lämna uppgiften till myndigheten i fråga. Det kan också finnas en skyldighet att lämna ut uppgiften till den andra myndigheten även om sekretess gäller för uppgiften under förutsättning att det finns en sekretessbrytande regel som är tillämplig i förhållande till den myndigheten.

Om man vill förhindra ett uppgiftsutbyte mellan myndigheter, är det alltså inte tillräckligt att införa en ny sekretessbestämmelse. Det måste också införas bestämmelser som föreskriver att de sekretessbrytande reglerna i 10 kap. OSL inte ska gälla.

Begränsningar i lag om en myndighets möjlighet att använda uppgifter från en myndighet i en annan stat

I 9 kap. 2 § OSL räknas ett antal lagar upp som innehåller bestämmelser som begränsar möjligheterna att använda vissa uppgifter som en svensk myndighet har fått från en myndighet i annan stat. Det rör sig bl.a. om lagen (1990:314) om ömsesidig handräckning i

skatteärenden, lagen (2000:343) om internationellt polisiärt samarbete och lagen (2000:344) om Schengens informationssystem.

Bestämmelsen utgjorde tidigare tredje stycket i dåvarande 1 kap. 4 § SekrL (numera 7 kap. 1 § OSL). I första stycket samma paragraf föreskrevs att om förbud gäller enligt denna lag mot att röja uppgift, får uppgiften inte heller i övrigt utnyttjas utanför den verksamhet i vilken sekretess gäller för uppgiften. I andra och tredje styckena fanns hänvisningar till olika lagar med bestämmelser om förbud mot eller begränsningar i möjligheten att utnyttja vissa uppgifter. Det tredje stycket infördes i samband med att lagen (1991:1342) med vissa bestämmelser om internationellt samarbete på brottmålsområdet infördes. I den lagen fanns bestämmelser som begränsade möjligheterna att utnyttja vissa uppgifter som en svensk myndighet har fått från en annan stat. I specialmotiveringen till bestämmelsen i det då nya tredje stycket i 1 kap. 4 § SekrL anfördes (prop. 1990/91:131 s. 26) att en av principerna bakom regleringen i sekretesslagen är att alla tystnadsplikter inom det allmännas verksamhet ska framgå av lagen antingen direkt eller genom en hänvisning till en annan lag. Myndigheterna skulle komma att omfattas av begränsningar i möjligheterna att utnyttja information enligt bestämmelserna i den nu föreslagna lagen om internationellt samarbete på brottmålsområdet. Det var därför naturligt att det av 1 kap. 4 § SekrL, där det redan fanns en hänvisning till insiderlagen och dess regler om förbud att utnyttja information, skulle framgå att ett förbud för myndigheter att utnyttja uppgifter också fanns i lagen med vissa bestämmelser om internationellt samarbete på brottmålsområdet.

Det kan konstateras att det ovan återgivna uttalandet är något missvisande i så måtto att bestämmelsen inte i sig innebär någon tystnadsplikt i den meningen att den föreskriver sekretess för vissa uppgifter, även om bestämmelsen i och för sig finns i offentlighets- och sekretesslagen. Däremot erinrar bestämmelsen om att det i andra lagar finns bestämmelser som begränsar svenska myndigheters möjlighet att använda vissa uppgifter. Dessa begränsningar gäller alltså oavsett om de omnämns i 9 kap. 2 § OSL. Det är således inte fråga om någon sådan hänvisning i offentlighets- och sekretesslagen till en annan lag som enligt 2 kap. 2 § TF kan utgöra hinder mot att lämna ut uppgiften enligt rätten att ta del av allmänna handlingar. Sådana begränsningar i möjligheten att använda vissa uppgifter som avses i

de lagar som räknas upp i 9 kap. 2 § OSL innebär alltså inte någon begränsning i den enskildes rätt att enligt 2 kap. TF att ta del av allmänna handlingar (Lenberg m.fl., kommentaren till 9 kap. 2 §).

Eftersom 9 kap. 2 § inte innebär att någon sekretess gäller utan enbart upplyser om att användningsbegränsningar finns i andra lagar, utgör sådana begränsningar inte heller något sekretesshinder som kan begränsa en myndighets informationsskyldighet gentemot en annan myndighet enligt 6 kap. 5 § OSL. Om det inte finns någon sekretessbestämmelse som är tillämplig på en uppgift som begärs ut av en annan myndighet eller om det finns en sekretessbrytande regel som kan tillämpas i förhållande till den myndigheten, ska uppgifterna alltså lämnas ut enligt 6 kap. 5 § OSL, såvida inte utlämnandet hindrar arbetets behöriga gång.

Begränsningar i att utnyttja vissa uppgifter enligt de lagar som räknas upp i 9 kap. 2 § OSL är emellertid i allmänhet utformade så att de inte enbart tar sikte på den svenska myndighet som tar emot uppgifter från en myndighet i en annan stat. I regel har bestämmelsen i den aktuella lagen utformats så att begränsningarna gäller för alla svenska myndigheter. Det får till följd att inte heller en annan svensk myndighet än den som fått uppgifterna från den utländska myndigheten kan utnyttja uppgifterna i sin verksamhet, även om myndigheten i och för skulle ha rätt att få ut dem efter en begäran enligt 6 kap. 5 § OSL. Det torde därför i praktiken bli aktuellt för en svensk myndighet att begära ut uppgifter som omfattas av användningsbegränsningar från en annan myndighet bara när myndigheten behöver ta del av uppgifterna för ett ändamål som inte omfattas av begränsningarna (jfr prop. 2012/13:4 s. 90 f.). I praktiken uppstår därför inte någon konflikt mellan lagbestämmelser om användningsbegränsningar och informationsskyldigheten enligt 6 kap. 5 § OSL.

Sammanfattningsvis kan det alltså konstateras att 9 kap. 2 § OSL inte i sig innebär något hinder mot att lämna ut uppgifter till en annan myndighet. I bestämmelsen erinras emellertid om att det i andra lagar finns bestämmelser som begränsar möjligheterna för svenska myndigheter att använda sig av uppgifter som ursprungligen kommer från en myndighet i en annan stat.

I sammanhanget kan påpekas att 9 kap. 2 § OSL enbart upplyser om användningsbegränsningar som finns i andra lagar. Det finns i och för sig inget som hindrar att regeringen meddelar föreskrifter

om begränsningar i möjligheterna att använda vissa uppgifter som en svensk myndighet har fått från en utländsk myndighet och som i så fall, på samma sätt som en bestämmelse i lag, blir bindande för alla myndigheter. I vilken utsträckning regeringen har meddelat sådana föreskrifter är inte känt för utredningen.

Den nya bestämmelsen om sekretess i det internationella samarbetet

Den 1 januari 2014 trädde en ny sekretessbestämmelse i kraft i syfte att utgöra en generellt tillämplig bestämmelse till skydd för uppgifter som utbyts inom ramen för Sveriges internationella relationer. Bestämmelsen har förts in i 15 kap. 1 a § OSL och innebär att sekretess gäller för en uppgift som en myndighet har fått från ett utländskt organ på grund av en bindande EU-rättsakt eller ett av EU ingånget eller av riksdagen godkänt avtal med en annan stat eller mellanfolklig organisation. Som en förutsättning för sekretess gäller att det kan antas att Sveriges möjlighet att delta i det internationella samarbete som avses i rättsakten eller avtalet försämras om uppgiften röjs. Motsvarande sekretess ska gälla för en uppgift som en myndighet har inhämtat i syfte att överlämna den till ett utländskt organ i enlighet med en sådan rättsakt eller ett sådant avtal.

Om sekretess gäller enligt bestämmelsen, får de sekretessbrytande bestämmelserna i 10 kap. 15–27 §§ och 28 § första stycket inte tillämpas (15 kap. 1 a § tredje stycket).

Bestämmelsens tillämpningsområde är alltså begränsat till uppgifter som en myndighet antingen har fått från ett utländskt organ eller har inhämtat i syfte att överlämna till ett sådant organ på grund av en bindande EU-rättsakt eller ett avtal som har ingåtts av EU eller av Sverige med en annan stat eller en mellanfolklig organisation. I det sistnämnda fallet gäller emellertid som förutsättning att riksdagen har godkänt avtalet. Sekretessbestämmelsen är således inte tillämplig på uppgifter som finns hos en myndighet på grund av internationella avtal som ingåtts av en förvaltningsmyndighet eller av regeringen utan godkännande av riksdagen. I förarbetena anfördes att en sådan ordning hade varit problematisk ur ett principiellt perspektiv för en sekretessbestämmelse med generell räckvidd (prop. 2012/13:192 s. 31). Regeringen hänvisade också till att några

remissinstanser hade ifrågasatt om en sådan bestämmelse hade varit förenlig med lagkravet i 2 kap. 2 § TF.

I offentlighets- och sekretesslagen finns flera bestämmelser som föreskriver sekretess i samband med vissa internationella samarbeten där något traditionellt skaderekvisit inte finns (se t.ex. 17 kap. 7 § andra stycket, 17 kap. 7 a § och 18 kap. 17 §). Enligt den nya bestämmelsen i 15 kap. 1 a § gäller emellertid ett rakt skaderekvisit. Den svenska myndigheten ska alltså göra en självständig bedömning av om ett utlämnande i det enskilda fallet kan antas försämra Sveriges möjligheter att delta i det aktuella samarbetet. I förarbetena påpekas att det inte finns något som hindrar den svenska myndigheten att vid sekretessprövningen kontakta den utlämnande utländska myndigheten för att utreda om sekretess bör gälla i det enskilda fallet. Om sekretess gäller för uppgifterna hos den utländska myndigheten är utgångspunkten typiskt sett att skaderekvisititet är uppfyllt (a. prop. s. 34 f.). Enligt regeringen kommer en tillämpning av sekretessbestämmelsen normalt inte att aktualiseras i sådana situationer då avtalet eller EU-rättsakten inte innehåller någon tydlig sekretessbestämmelse, även om en sådan inte utesluts av dess ordalydelse. Regeringen anser att det då ligger närmare till hands att tillämpa bestämmelsen om utrikessekretess i 15 kap. 1 § OSL. Bestämmelser i EU-rättsakter eller internationella avtal om begränsningar i för vilka ändamål uppgifter får användas, dvs. den typen av begränsningar som 9 kap. 2 § OSL tar sikte på, bör enligt regeringen inte heller aktualisera en tillämpning av den nya sekretessbestämmelsen (a. prop. s. 35).

I förarbetena till den nya sekretessbestämmelsen för informationsutbyte vid internationellt samarbete i 15 kap. 1 a § OSL finns en utförlig beskrivning av överenskommelser om sådant utbyte som kan finnas i avtal och EU-rättsakter (prop. 2012/13:192 s. 10 f.). Vi hänvisar till den redovisningen och lämnar alltså inte någon egen redovisning här.

6.2 Våra överväganden

Bedömning: Det finns inte något tillräckligt stort behov av att ändra 6 kap. 5 § OSL så att paragrafen står i bättre överensstämmelse med användningsbegränsningar som kan förekomma i samband med internationella åtaganden.

6.2.1 Behovet av en ny bestämmelse

I våra direktiv konstateras att 9 kap. 2 § OSL visserligen ger en upplysning om att användningsbegränsningar införts i vissa andra författningar. Det påpekas att uppräkningen emellertid inte är heltäckande och att det inte finns någon formell koppling mellan den bestämmelsen och 6 kap. 5 § OSL (jfr prop. 1990/91:131 s. 25). Den beskrivna frågeställningen har enligt regeringen en sådan betydelse för uppgiftsutbytet mellan myndigheter att det bör övervägas om 6 kap. 5 § OSL bör justeras så att den står i bättre överensstämmelse med förekomsten av nu nämnda användningsbegränsningar.

Vår uppgift i denna del är inte att överväga behovet av en ny sekretessbestämmelse som kan hindra utlämnanden både till enskilda, med stöd av 2 kap. TF eller på annan grund, och till myndigheter. Uppdraget avser enbart att överväga en eventuell begränsning som kan utgöra hinder för en myndighet att lämna uppgifter till en annan myndighet.

Betydelsen av uppräkningen i 9 kap. 2 § OSL

Bestämmelsen i 9 kap. 2 § OSL erinrar om att det i andra lagar finns bestämmelser som begränsar en svensk myndighets användning av vissa uppgifter. Uppräkningen i paragrafen av lagar där sådana användningsbegränsningar finns utgör alltså en upplysning och syftar inte till att i sig reglera något. Sådana begränsningar gäller alltså för svenska myndigheter till följd av regleringen i den särskilda lagen och inte på grund av att sådana lagar räknas upp i 9 kap. 2 § OSL. Att uppräkningen i 9 kap. 2 § OSL inte är uttömmande har således inte någon betydelse för om en myndighet är skyldig att följa en sådan användningsbegränsning eller inte. Däremot kan det vara svårt

för myndigheter att hålla reda på de användningsbegränsningar som gäller enligt särskilda lagar, om de inte finns samlade på något sätt.

Det kan emellertid konstateras att om en användningsbegränsning har reglerats i en lag på ett sådant sätt att den gäller för alla svenska myndigheter, förefaller det knappast finnas något praktiskt behov av att justera 6 kap. 5 § OSL så att den paragrafen också hindrar ett utlämnande av uppgifter till en annan myndighet på grund av en sådan användningsbegränsning. Som påpekats i flera lagstiftningsärenden torde det inte bli aktuellt för en myndighet att begära ut uppgifter från en annan myndighet med stöd av 6 kap. 5 § OSL om man ändå inte får använda sig av uppgifterna. I dessa fall har det ansetts tillräckligt i praktiken att användningsbegränsningen gäller enligt den särskilda lagen. Något faktiskt behov av att justera 6 kap. 5 § OSL så att paragrafen kan sägas bättre stå i överensstämmelse med förekomsten av sådana särskilt reglerade användningsbegränsningar förefaller alltså inte finnas. Däremot saknas alltså, som påpekas i våra direktiv, en formell koppling mellan 6 kap. 5 § OSL och sådana svenska författningsbestämmelser som begränsar en myndighets möjlighet att använda vissa uppgifter som inhämtats genom ett internationellt informationsutbyte.

Som redan påpekats har det ingen betydelse för frågan om en användningsbegränsning gäller för en myndighet eller inte om den särskilda lag där begränsningen föreskrivs räknas upp i 9 kap. 2 § OSL. Däremot skulle en komplett sådan uppräkning naturligtvis innebära en bättre möjlighet för myndigheter att själva hålla reda på i vilka situationer användningsbegränsningar gäller.

Användningsbegränsningar i EU-rättsliga lagstiftningsakter

I våra direktiv nämns att sektorspecifika EU-rättsakter kan innehålla artiklar om att en myndighet bara får använda uppgifter som erhålls enligt rättsakten för vissa angivna ändamål eller i viss verksamhet.

Om det är frågan om en EU-förordning gäller den för svenska myndigheter utan att dess artiklar behöver genomföras i svensk rätt genom inhemsk lagstiftning. I den mån en EU-förordning innehåller sådana användningsbegränsningar som gäller för alla myndigheter finns således inte, i likhet med vad som gäller användnings-

begränsningar i särskilda lagar, något praktiskt behov av att göra en justering av 6 kap. 5 § OSL. Inte heller i dessa fall torde det ju bli aktuellt för en myndighet att begära ut uppgifter som omfattas av en sådan användningsbegränsning, eftersom myndigheten ändå inte får använda sig av uppgifterna.

Om användningsbegränsningar finns i ett EU-direktiv i stället för i en förordning, måste direktivet genomföras i svensk rätt genom inhemsk lagstiftning i den mån direktivet inte kan anses gälla redan enligt svenska regler. Användningsbegränsningar som gäller enligt ett EU-direktiv kommer alltså till uttryck genom en svensk författning. Sådana användningsbegränsningar kan därigenom komma att gälla för alla svenska myndigheter. Inte heller i ett sådant fall finns det alltså något praktiskt behov av att justera 6 kap. 5 § OSL.

Det förtjänar att påpekas att några av de särskilda lagar som räknas upp i 9 kap. 2 § OSL är lagar som har införts för att genomföra ett EU-direktiv. Som exempel kan nämnas lagen (2012:843) om administrativt samarbete inom Europeiska unionen i fråga om beskattning.

Användningsbegränsningar som inte är författningsreglerade

Det förekommer att EU beslutar andra bindande rättsakter än lagstiftningsakter i form av delegerade akter och genomförandeakter (se t.ex. prop. 2012/13:192 s. 43). EU ingår också avtal med tredje land för medlemsstaternas räkning genom sin på vissa områden exklusiva kompetens, exempelvis på det handelspolitiska området. I andra fall ingår respektive land för egen del bilaterala avtal med en utländsk aktör. Ibland är det då fråga om s.k. blandade avtal, där EU också för egen del har träffat avtal. Så är fallet exempelvis när det gäller avtal som träffas inom ramen för WTO, där både medlemsstaterna och EU är medlemmar. Ett annat exempel är frihandelsavtal som träffas med en del tredjeländer (se vidare a. prop. s. 10). Svenska myndigheter kan också träffa internationella avtal som behandlar frågor om informationsutbyte.

En bindande EU-rättsakt som inte är en lagstiftningsakt är bindande för Sverige såsom medlemsstat, men innebär inte i sig att rättsakten måste komma till uttryck i svensk lagstiftning eller på annan grund tillämpas av svenska myndigheter. Ett internationellt avtal som EU eller Sverige för egen del eller en svensk myndighet

träffar kan innehålla bestämmelser som reglerar frågor om informationsutbyte. Om bestämmelser som reglerar informationsutbyte i ett avtal inte har kommit till uttryck i någon svensk föreskrift utan endast i avtalet, kan de bestämmelserna inte binda någon annan än den som har ingått avtalet. Det innebär att om EU har ingått avtalet är det bindande för Sverige antingen direkt eller efter att det ratificerats av Sverige, eventuellt efter godkännande av riksdagen. Det är då bindande för Sverige som stat i folkrättslig bemärkelse, men gäller inte direkt för svenska myndigheter. Detsamma gäller för sådana internationella avtal som Sverige för egen del ingår. Om ett avtal har ingåtts av en svensk myndighet är avtalet enbart bindande för den myndigheten. Ett avtal som har ingåtts av EU, av Sverige som stat eller av en svensk myndighet är alltså inte bindande för samtliga svenska myndigheter. Om det innehåller bestämmelser som innebär begränsningar i att använda uppgifter, är andra svenska myndigheter än den som mottagit uppgiftena från den utländska aktören således inte skyldiga att följa bestämmelserna.

Eftersom alla myndigheter inte är skyldiga att iaktta användningsbegränsningar som enbart kommit till uttryck i en bindande EU-rättsakt som inte är en lagstiftningsakt eller i ett avtal, finns det inget praktiskt hinder för en myndighet att begära ut uppgifter från en annan myndighet som för egen del har att iaktta sådana begränsningar enligt EU-rättsakten eller det internationella avtalet. I det fallet finns det alltså i praktiken inget som hindrar den myndighet som begär ut uppgifterna att också använda dem. Det kan då uppfattas som ett problem att en myndighet, som eventuellt själv har ingått avtalet i fråga, och tagit emot uppgifter från en utländsk aktör på de villkor som angetts i ett internationellt avtal, saknar möjlighet att iaktta de användningsbegränsningar som angetts i avtalet om en annan myndighet begär ut uppgifter med stöd av 6 kap. 5 § OSL. För denna situation kan det alltså anses finnas ett praktiskt behov – inte bara ett formellt sådant – av att justera 6 kap. 5 § OSL så att den bestämmelsen generellt kan förhindra att uppgifter lämnas ut till en myndighet i sådana situationer där användningsbegränsningar av det nu aktuella slaget föreligger.

6.2.2 Hur kan 6 kap. 5 § OSL justeras?

Bestämmelser om användningsbegränsningar i föreskrifter som svenska myndigheter är skyldiga att följa

I våra direktiv påtalas att det är ett problem att det inte finns någon formell koppling mellan 6 kap. 5 § och 9 kap. 2 § OSL. Tanken bakom detta synes vara att om en sådan formell koppling kan åstadkommas skulle användningsbegränsningar som finns i de lagar som räknas upp i paragrafen begränsa, liksom sekretess, den informationsskyldighet i förhållande till en annan myndighet som annars gäller enligt 6 kap. 5 § OSL.

Om syftet är att alla användningsbegränsningar som kommit till uttryck i en svensk lag också ska innebära att det finns ett hinder mot att lämna ut uppgifterna enligt 6 kap. 5 § OSL kan man emellertid sätta i fråga om det är tillräckligt att åstadkomma en formell koppling mellan 6 kap. 5 § och 9 kap. 2 §. Som framgår av redovisningen ovan reglerar inte 9 kap. 2 § i sig frågan om en uppgift kan användas eller inte i en viss verksamhet. Den bestämmelsen innehåller enbart upplysningar om att det finns andra lagar som innehåller bestämmelser om sådana användningsbegränsningar. I våra direktiv konstateras att uppräkningen inte är uttömmande. Vi har för egen del inte undersökt i vilken omfattning det förekommer lagar med bestämmelser om sådana användningsbegränsningar som inte finns med i uppräkningen i 9 kap. 2 § OSL.

Ett annat problem med 9 kap. 2 § OSL, dvs. förutom att paragrafen inte på ett fullständigt sätt räknar upp de lagar där bestämmelser om användningsbegränsningar finns, är att den inte heller upplyser om att användningsbegränsningar finns i vissa EU-förordningar. Om bestämmelser om användningsbegränsningar finns i sådana förordningar kan svenska myndigheter vara skyldiga att följa dem när det gäller uppgiftsutbyte med andra myndigheter på samma sätt som användningsbegränsningar som föreskrivits i en svensk lag.

Som framgår av redovisningen ovan kan det inte anses innebära något praktiskt problem att det saknas en formell koppling mellan 6 kap. 5 § och 9 kap. 2 § OSL, eftersom det saknas skäl för en myndighet att begära ut uppgifter från en annan myndighet som den ändå inte får använda. I dessa fall uppstår det alltså normalt inte någon sådan situation där en myndighet måste uppfylla sin informationsskyldighet enligt 6 kap. 5 § OSL. Om man ändå anser att

det finns ett behov av att formellt säkerställa att en myndighet inte ska behöva lämna ut uppgifter i de fall då användningsbegränsningar finns enligt uppräkningen i 9 kap. 2 § OSL och inför en sådan bestämmelse i 6 kap. 5 §, innebär det att en konflikt mellan dessa bestämmelser inte längre finns. Däremot skulle en regelkonflikt kvarstå mellan 6 kap. 5 § OSL och övriga föreskrifter som innebär att svenska myndigheter är skyldiga att följa användningsbegränsningar, dvs. då sådana föreskrifter finns i EU-förordningar samt i lagar som inte räknas upp i 9 kap. 2 § OSL. Detsamma gäller för det fall det skulle vara så att regeringen i något eller några fall har meddelat föreskrifter om sådana användningsbegränsningar.

Att åstadkomma en formell koppling mellan 6 kap. 5 § och 9 kap. 2 § OSL leder alltså endast till en viss förbättrad systematik i formellt hänseende. Det löser emellertid inte hela den konflikt som kan uppfattas finnas mellan svenska regler som å ena sidan säger att en myndighet har rätt att få ut uppgifter från en annan myndighet, medan andra regler föreskriver att myndigheten inte får använda uppgifterna. För att denna konflikt helt ska lösas bör i stället 6 kap. 5 § OSL formellt kopplas direkt till bestämmelser om användningsbegränsningar snarare än till 9 kap. 2 § OSL. Om man ändå skulle överväga en koppling till den senare bestämmelsen måste paragrafen kompletteras så att den på ett uttömmande sätt upplyser om samtliga användningsbegränsningar som svenska myndigheter är skyldiga att följa.

Bestämmelser om användningsbegränsningar som inte är bindande för alla myndigheter

Som har framgått finns det EU-rättsakter som visserligen är bindande för Sverige som medlemsstat, men inte är lagstiftningsakter som måste tillämpas av svenska myndigheter på grund av att de genomförts i svensk lagstiftning eller på annan grund. Om de innehåller bestämmelser om användningsbegränsningar gäller de alltså inte för alla myndigheter. Ett internationellt avtal som EU eller Sverige för egen del eller en svensk myndighet träffar kan också innehålla bestämmelser som reglerar frågor om informationsutbyte. Om sådana bestämmelser inte har kommit till uttryck i någon svensk föreskrift utan endast i avtalet, kan de bestämmelserna inte binda någon annan än den som har ingått avtalet. De gäller alltså i

så fall inte för alla svenska myndigheter, utan endast för den svenska myndighet som tar emot uppgifter från den utländska aktören.

När det gäller denna typ av användningsbegränsningar finns det alltså inte någon konflikt mellan svenska författningsbestämmelser som å ena sidan säger att uppgifter ska lämnas ut till en annan myndighet och å andra sidan att den myndigheten inte får använda uppgifterna. I detta fall finns ju inte några svenska bestämmelser som innebär begränsningar i möjligheterna för alla myndigheter att använda sig av uppgifter som härrör från det internationella informationsutbytet. Däremot kan det uppfattas finnas en konflikt mellan informationsskyldigheten enligt 6 kap. 5 § OSL och de åtaganden som Sverige som stat eller som medlemsstat i EU eller som en svensk myndighet har gjort i ett internationellt samarbete, om den svenska parten i ett sådant samarbete har åtagit sig att se till att uppgifter som en svensk myndighet kan få genom samarbetet endast ska användas för vissa ändamål.

Ett sätt att lagstiftningsvägen lösa den konflikt som nu är i fråga skulle kunna vara att föra in en bestämmelse i 6 kap. 5 § OSL som innebär att en myndighet är förhindrad att lämna ut en uppgift till en annan myndighet, om myndigheten har fått uppgiften genom ett internationellt samarbete på villkor att uppgifterna endast får användas för vissa ändamål. Det som skiljer detta fall från situationen ovan är att den myndighet som begär att få uppgifter med stöd av 6 kap. 5 § OSL inte är förbjuden att använda sig av uppgifterna enligt någon författningsbestämmelse. En ny föreskrift i 6 kap. 5 § OSL som hindrar ett utlämnande i dessa situationer skulle alltså inte enbart ta sikte på den formella frågan utan skulle innebära en reell inskränkning i myndigheters informationsskyldighet enligt 6 kap. 5 § OSL.

Om det införs en föreskrift i 6 kap. 5 § OSL som generellt hänvisar till användningsbegränsningar som har kommit till uttryck i ett internationellt samarbete som Sverige som stat eller en svensk myndighet deltar i, dvs. oavsett om begränsningarna också kommit till uttryck i en föreskrift som alla myndigheter är skyldiga att följa, innebär det exempelvis att en svensk myndighet skulle kunna avtala om villkor som får till effekt att informationsskyldigheten i 6 kap. 5 § OSL inskränks. En sådan ordning kan anses problematisk från principiella utgångspunkter. I sammanhanget kan nämnas att den nya generella sekretessbestämmelsen i 15 kap. 1 a § OSL om sekre-

tess i det internationella samarbetet har avgränsats så att om en myndighet har fått en uppgift på grund av ett internationellt avtal, är bestämmelsen endast tillämplig om avtalet har ingåtts av EU eller godkänts av riksdagen. I förarbetena anfördes att detta innebar en väsentlig inskränkning av bestämmelsens tillämpningsområde och skulle i praktiken göra att sekretess för uppgifter som utbyts enligt ett visst avtal endast skulle primärt komma att gälla hos ett begränsat och överblickbart antal myndigheter (prop. 2012/13:192 s. 32). Det finns emellertid även bestämmelser om sekretess till följd av internationella avtal som inte uppställer något krav på att avtalet ska ha godkänts av riksdagen. Enligt exempelvis 30 kap. 7 § första stycket andra meningen OSL gäller sekretess hos Finansinspektionen för uppgifter som inspektionen har fått från en utländsk myndighet eller ett utländskt organ enligt ett avtal. Som förutsättning gäller emellertid att regeringen har meddelat föreskrifter om detta (se 8 § offentlighets- och sekretessförordningen).

6.2.3 Vår bedömning

I de fall det finns bestämmelser om användningsbegränsningar enligt en EU-förordning eller en svensk författningsbestämmelse sker i normalfallet i praktiken inte något uppgiftsutbyte på grund av informationsskyldigheten enligt 6 kap. 5 § OSL. Skälet till det är, som redovisats ovan, att myndigheter inte begär ut uppgifter från en annan myndighet med stöd av den bestämmelsen om de ändå inte får använda uppgifterna. I dessa fall förefaller det alltså inte finnas något reellt behov av att justera 6 kap. 5 § OSL för att undvika en konflikt med internationella åtaganden. Vi kan emellertid inte se att det skulle finnas några systematiska eller liknande skäl som talar emot att 6 kap. 5 § OSL justeras så att man åstadkommer en formell koppling mellan den bestämmelsen och andra bestämmelser om användningsbegränsningar, vilka myndigheterna ändå är skyldiga att följa.

Det förefaller däremot inte ändamålsenligt att åstadkomma en formell koppling mellan 6 kap. 5 § och 9 kap. 2 § OSL, eftersom det inte skulle innebära att samtliga fall då det finns bestämmelser som begränsar myndigheters möjlighet att använda vissa uppgifter fångas upp.

Den nya bestämmelsen om sekretess i samband med internationellt samarbete i 15 kap. 1 a § OSL har avgränsats så att den enbart ska tillämpas på uppgifter som utbyts på grund av en bindande EU-rättsakt eller ett avtal som har ingåtts av EU eller av riksdagen godkänt avtal med en annan stat eller en mellanfolklig organisation. Som har framgått anfördes som skäl för denna avgränsning bl.a. att en ordning där uppgifter som finns hos en myndighet på grund av andra internationella avtal än sådana som har godkänts av riksdagen också skulle omfattas av den nya sekretessbestämmelsen skulle vara problematisk ur ett principiellt perspektiv för en bestämmelse med generell räckvidd. Några remissinstanser hade också satt i fråga om en sådan bestämmelse hade varit förenlig med lagkravet enligt 2 kap. 2 § TF.

Den bestämmelse som nu är i fråga i 6 kap. 5 § OSL innebär visserligen inte några begränsningar av den grundlagsstadgade rätten för var och en att ta del av allmänna handlingar utan reglerar enbart utbytet av uppgifter mellan myndigheter. Det kan emellertid konstateras att det svenska förvaltningsrättsliga systemet bygger på att myndigheter så långt möjligt ska samverka, även när det gäller utbyte av information (jfr 6 § FL). Regleringen bygger på principen att det är en fråga för lagstiftaren att avgöra när en sådan skyldighet ska finnas. Det bör således inte vara upp till den enskilda myndigheten att bedöma när information som myndigheten har tillgång till ska utbytas med en annan myndighet. Om 6 kap. 5 § OSL skulle justeras på ett sådant sätt att det generellt skulle finnas ett hinder mot att lämna ut uppgifter till andra myndigheter då det inom ramen för ett internationellt informationsutbyte har uppställts villkor om användningsbegränsningar, dvs. även om dessa begränsningar inte har kommit till uttryck i en föreskrift utan enbart i ett avtal som en enskild myndighet har slutit, skulle emellertid en enskild myndighet ha befogenhet att själv styra över vad den ska dela med sig av till andra myndigheter av den information som den fått genom ett internationellt avtal. Enligt vår uppfattning skulle en sådan ordning få alltför långtgående och principiellt betänkliga effekter. En bestämmelse med en sådan innebörd bör alltså inte införas. I sammanhanget kan det konstateras att det i och för sig saknas hinder för regeringen att genom en föreskrift bestämma att användningsbegränsningar som enbart kommit till uttryck i ett

internationellt avtal mellan exempelvis en svensk myndighet och en utländsk myndighet också ska gälla för andra myndigheter.

När det gäller andra bindande EU-rättsakter än lagstiftningsakter samt avtal som ingåtts av EU eller Sverige har vi inte erfarit att det i sådana sammanhang förekommer regler eller villkor om användningsbegränsningar i en sådan omfattning att detta påkallar en begränsning av informationsskyldigheten enligt 6 kap. 5 § OSL.

Sammanfattningsvis kan alltså konstateras att i fråga om bestämmelser om användningsbegränsningar i en EU-förordning eller en svensk författningsbestämmelse det saknas ett praktiskt behov av att ändra 6 kap. 5 § OSL. Det finns vidare principiella betänkligheter mot att ändra 6 kap. 5 § OSL så att användningsbegränsningar som inte kommit till uttryck i en föreskrift utan enbart i ett avtal som en enskild myndighet har slutit skulle begränsa informationsskyldigheten i förhållande till andra myndigheter. När det gäller andra bindande EU-rättsakter än lagstiftningsakter samt avtal som EU eller Sverige ingår har vi inte erfarit att det finns något påtagligt behov av en lagändring.

Vi lämnar därför inte något förslag till en ändring av 6 kap. 5 § OSL.

I den händelse det ändå bedöms finnas ett behov av en sådan ändring förordar vi att den enbart tar sikte på att åtgärda det formella behov av en ändring som kan uppfattas finnas i fråga om bestämmelser om användningsbegränsningar i en EU-förordning eller en svensk författningsbestämmelse. I så fall skulle 6 kap. 5 § OSL kunna ges följande lydelse:

> En myndighet ska på begäran av en annan myndighet lämna uppgift som den förfogar över, om inte uppgiften är sekretessbelagd *eller inte får användas av den andra myndigheten enligt lag eller förordning. En uppgift behöver inte heller lämnas* om det skulle hindra arbetets behöriga gång.

Med uttrycket att en myndighet inte får använda uppgiften enligt lag avses också en bestämmelse i en EU-förordning (se prop. 1999/2000:126 s. 272 och 283).

Vi vill avslutningsvis framhålla att det under alla förhållanden inte kan anses vara en tillfredsställande ordning att uppräkningen av lagar med bestämmelser om användningsbegränsningar i 9 kap. 2 § OSL inte är fullständig. Om bestämmelsen ska kunna fylla sin funktion att upplysa om sådana användningsbegränsningar bör uppräk-

ningen givetvis vara komplett. Vi har emellertid inte sett det som en uppgift för oss att komplettera uppräkningen i bestämmelsen.

EN NY LAG OM MYNDIGHETERS BEHANDLING AV PERSONUPPGIFTER

7 En generell reglering – utgångspunkter och inledande ställningstaganden

7.1 Allmänna utgångspunkter

7.1.1 Uppdraget

Det övergripande uppdraget enligt våra direktiv (dir. 2011:86) är alltså att se över den s.k. registerlagstiftningen i syfte att skapa rättsliga förutsättningar för en mer effektiv e-förvaltning, där såväl den enskildes rätt till personlig integritet som allmänhetens berättigade anspråk på insyn i den offentliga förvaltningen tillgodoses. Utredningens förslag ska syfta till att regleringen i tryckfrihetsförordningen och offentlighets- och sekretesslagen (2009:400) samt registerregleringen tillsammans inom respektive område ska utgöra en tydligare och mer lättillämpad helhet.

I direktiven pekas vidare på det problematiska i om de grundläggande reglerna i tryckfrihetsförordningen och offentlighets- och sekretesslagen samt den principiella uppbyggnaden av registerförfattningarna inte är anpassade till varandra. Det blir då svårt att i ett enskilt lagstiftningsärende om elektronisk informationsöverföring mellan två eller flera myndigheter hitta en lösning som är tillfredsställande från integritets-, effektivitets- och öppenhetssynpunkt. För att ytterligare kunna effektivisera förvaltningen med modern informationsteknik är det därför viktigt dels att respektive regelverk bör vara väl genomtänkta och så enkla som möjligt att tillämpa, dels att regelverken bör vara förenliga med varandra.

Den anvisade metoden för att åstadkomma genomtänkta regelverk som är lätta att tillämpa och som sinsemellan så långt möjligt är förenliga är enligt tilläggsdirektiv (dir. 2014:31) att utreda förut-

sättningarna för att skapa en generell, enhetlig och – helt eller i vart fall delvis – samlad reglering för myndigheternas behandling av personuppgifter. Tanken är att en sådan samlad reglering också är mer ändamålsenlig för att kunna möta den förändring som förmodligen kommer att ske inom EU genom en förordning som ersätter dataskyddsdirektivet. En samlad reglering kan fungera som ett komplement till eller, vid behov, genomföra delar av den unionsrättsliga regleringen på området. Vidare framhålls i direktiven att det också behöver göras en bedömning av vilket utrymme förordningen ger för att i nationell rätt göra undantag från förordningens bestämmelser för myndigheternas personuppgiftsbehandling.

Om vi bedömer att det finns förutsättningar att skapa en sådan samlad reglering, ska vi enligt direktiven lämna de författningsförslag som kan anses motiverade. Personuppgiftsbehandlingen inom den brottsbekämpande sektorn omfattas inte av utredningsuppdraget, eftersom den behandlingen inte omfattas av kommissionens förslag till en allmän uppgiftsskyddsförordning utan av ett förslag till ett direktiv.

Av våra direktiv följer vidare att vi ska överväga hur en generell reglering bör utformas utifrån vad som är lämpligt från bl.a. normgivningstekniska och systematiska utgångspunkter. I direktiven påpekas att även om personuppgiftsbehandling inom den brottsbekämpande verksamheten undantagits från utredningens arbete, behöver man vid utformningen av en ny reglering emellertid ta hänsyn till hur regleringen på såväl detta som andra områden är utformad för att regelverken inte ska komma i konflikt med varandra. Den generella regleringen bör om möjligt vara utformad så att den kan tillämpas på ett enhetligt sätt av myndigheter vars verksamhet i vissa delar kommer att omfattas av tillämpningsområdet för uppgiftsskyddsförordningen och i andra delar omfattas av tillämpningsområdet för EU-direktivet för den brottsbekämpande sektorn.

Av direktiven framgår slutligen att vi i vårt arbete noga ska följa den fortsatta behandlingen inom EU av förslaget till reformerad dataskyddsreglering. De förslag till författningsreglering som lämnas ska vara väl anpassade till denna översyn och dess resultat.

7.1.2 Förutsättningarna för en generell reglering

Automatiserad behandling är en integrerad del av myndigheters verksamhet

När personuppgiftslagen trädde i kraft den 24 oktober 1998 var den elektroniska förvaltningen fortfarande i början av sin uppbyggnad. I prop. 1997/98:136 En statlig förvaltning i medborgarnas tjänst redovisade regeringen ett handlingsprogram för bl.a. förvaltningens informationsförsörjning. Enligt detta program borde förvaltningen, med beaktande av integritets- och säkerhetsaspekter ta tillvara informationsteknikens möjligheter att förenkla och förbättra kontakterna för medborgare och företag med myndigheterna, öka allmänhetens insyn i och kontroll av myndigheternas verksamhet, effektivisera samverkan mellan myndigheter, med övrig offentlig sektor samt med EU-institutioner och andra länders förvaltning (a. prop. s. 54 f.). I programmet slogs vidare fast att den tekniska infrastrukturen för statsförvaltningens kommunikation med medborgare och företag borde bygga på internet, statliga myndigheter borde använda säker överföring av dokument och meddelanden i den öppna it-infrastrukturen samt att myndigheter vars verksamhet riktar sig främst till företag och medborgare borde erbjuda elektroniska tjänster för självbetjäning som komplement till traditionella tjänster. Regeringen uttalade också att en enkel, säker och kostnadseffektiv tillgång till samhällets grundläggande information är ett offentligt åtagande av väsentlig betydelse för den offentliga förvaltningen, för medborgarna och för företagen.

I dag är en elektronisk förvaltning en självklarhet för varje myndighet, statlig som kommunal. Handlingar framställs inom en myndighets verksamhet i princip uteslutande i elektronisk form och lagring sker på både kort och på lång sikt elektroniskt, även om det också förekommer lagring i pappersform. Ärenden handläggs elektroniskt och beslut fattas inom vissa myndigheters verksamhet, t.ex. Försäkringskassan och Skatteverket, i stor omfattning med beslutsstöd i automatiserad form. Handlingar kommer också in till myndigheterna på elektronisk väg i stor omfattning och expedieras från myndigheterna på samma sätt i allt högre grad. Arbetet med att öka effektiviteten i myndigheternas verksamhet och samverkan mellan myndigheterna samt att ge medborgarna en förbättrad service är i princip helt inriktat på att detta ska ske på elektronisk väg.

Det finns därför anledning att fråga sig om det fortfarande finns skäl att tala om en elektronisk förvaltning. Den elektroniska förvaltningen är ju inte längre någon särskild del av myndigheternas verksamhet, utan utgör i själva verket förvaltningen.

Användning av it genomsyrar i dag en myndighets hela verksamhet och utgör således basen för framställning av dokument, ärendehantering, lagring, kommunikation och samverkan. På motsvarande sätt kan myndigheternas automatiserade behandling av personuppgifter beskrivas, dvs. sådan behandling utgör det sätt på vilket myndigheterna hanterar personuppgifter. Vid tiden för personuppgiftslagens införande fanns det emellertid fortfarande anledning att tala om s.k. manuell hantering av personuppgifter, t.ex. för att handlägga ett ärende, som ett alternativ till automatiserad behandling. Detta betraktelsesätt har länge präglat lagstiftning som rör behandling av personuppgifter. I dag är den automatiserade behandlingen av personuppgifter alltså inte en del av en myndighets verksamhet som utförs åtskild från verksamheten i övrigt och därför kräver andra regler än de som i övrigt reglerar verksamheten. Däremot är det självfallet så att användningen av it fortfarande innebär att särskilda integritetsaspekter måste beaktas, bl.a. i form av regler om skydd för personuppgifter. Den elektroniska hanteringen medför också att myndigheterna behöver ta särskild hänsyn till säkerhetsaspekter, beträffande såväl personuppgifter som annan information som finns hos myndigheterna.

7.1.3 En generell reglering?

Bedömning: Vi menar att det finns förutsättningar för en samlad reglering beträffande myndigheters behandling av personuppgifter och vi kan inte se några bärande skäl som talar emot att en sådan nu införs.

Det brukar anföras som skäl för att införa särskilda registerlagar att man på så sätt åstadkommer en heltäckande, tydlig och uttömmande reglering av vad som ska gälla i fråga om personuppgiftsbehandling hos en viss myndighet eller inom en viss samhällssektor. Det ligger uppenbarligen ett värde i detta. Samtidigt är det

tydligt att det finns klara nackdelar förenade med den regleringsmodellen.

Som vi har berört i avsnitt 4.3.2 – och som vi närmare kommer att redovisa i följande kapitel – finns det ett antal generella problem förenade med det svåröverblickbara och fragmenterade rättsområde som registerlagstiftningen har kommit att bli. Registerförfattningarna har kommit att utformas utan tillräcklig inre konsekvens och enhetlighet i fråga om struktur, normtekniska lösningar eller beträffande hur enskilda kategorier av bestämmelser har utformats. Med tiden har detta bl.a. medfört relativt stora tillämpningsproblem i olika avseenden, inte minst vid uppgiftsutbyten mellan myndigheter. Samtidigt finns det påfallande många likheter mellan registerförfattningarna – inte minst beträffande de vi kallar informationshanteringsförfattningar – när det t.ex. gäller vilka slags frågor som regleras, varianter på begrepp och normtekniska lösningar. Det är i hög grad fråga om ”dubbelreglering” i den meningen att likartade bestämmelser finns intagna i ett stort antal författningar.

Ett annat problem med den nuvarande dataskyddsregleringen – och som gäller i lika hög grad även för de myndigheter som inte omfattas av någon registerförfattning utan enbart tillämpar personuppgiftslagen – är att tillräcklig uppmärksamhet inte ägnats åt anpassningen av dataskyddsregleringen till annan central reglering för myndigheters verksamhet och informationshantering. Myndigheters personuppgiftsbehandling skiljer sig nämligen på ett markant sätt från vad som normalt gäller i enskilda verksamheter. En myndighet som behandlar personuppgifter i sin verksamhet har inte bara att följa personuppgiftslagen eller en eventuell registerförfattning i sin informationshantering. Myndigheters personuppgiftsbehandling sker i verksamheter som är författningsreglerade, oftast i fråga om såväl vad som ska göras som hur det ska göras. Dessutom styrs personuppgiftsbehandlingen parallellt av annan central reglering för myndigheternas informationshantering än den dataskyddsrättsliga, bl.a. reglerna om handlingsoffentlighet och sekretess samt förvaltningslagen. Med ett fåtal undantag är personuppgiftslagens bestämmelser inte anpassade till dessa särskilda förhållanden.

Inom ramen för en samlad reglering skulle det finnas förutsättningar att åstadkomma den enhetlighet och konsekvens i regleringen av myndigheternas personuppgiftsbehandling som den nuvar-

ande splittrade regleringen saknar. Genom en samlad reglering skulle det vidare finnas förutsättningar att på ett betydligt mer ändamålsenligt sätt beakta de särskilda förutsättningar som gäller beträffande personuppgiftsbehandling på myndighetsområdet. Därtill kommer att en samlad reglering skulle i betydande mån minska det framtida behovet av att behålla eller införa nya sektorspecifika bestämmelser. Viss särreglering kommer givetvis att behövas även med en generell reglering men kan då utformas som särbestämmelser som innehåller undantag från huvudregler. Regelmassan vad gäller dataskyddsbestämmelser skulle alltså totalt sett minska väsentligt.

Genom att regelverket blir tydligare i den meningen att det klargörs vad som utgör ett berättigat dataskydd och hur detta ska åstadkommas på myndighetsområdet, främjas skyddet för personuppgifter. Samtidigt ger ett sådant regelverk klarare besked om i vilken utsträckning dataskyddshänsyn *inte* påverkar övriga regelverk som reglerar myndigheternas verksamhet och de intressen som där värnas. En tydligare dataskyddsreglering på myndighetsområdet innebär t.ex. att förhållandet mellan dataskyddsregler och regler om sekretess blir klarare, vilket som vi ser det kommer att vara till gagn för offentlighet och insyn. En tydligare reglering ökar också i betydande grad förutsättningarna för att anpassa offentlighetsprincipen till moderna elektroniska kommunikationsformer. Huvudambitionen att på ett mer effektivt sätt tillgodose allmänhetens berättigade anspråk på insyn i den offentliga förvaltningen uppfylls därför också genom den generella regleringen.

Vi kan för vår del inte se några bärande skäl som talar mot en generell reglering beträffande myndigheters behandling av personuppgifter. Vi menar alltså att det finns förutsättningar för en sådan samlad reglering.

En utgångspunkt för arbetet med en generell reglering om myndigheters behandling av personuppgifter bör vara att den inte till någon del ska syfta till att reglera en myndighets verksamhet. Regleringen bör i stället utformas så att den enbart tar sikte på att reglera dataskyddsrättsliga frågor, dvs. i första hand frågor rörande det behov av skydd för enskilda registrerades personliga integritet som den automatiserade behandlingen av personuppgifter ger upphov till. Förändringar som sker beträffande myndigheters faktiska, organisatoriska eller rättsliga förutsättningar ska därmed inte ha betydelse på det sättet att innehållet i den generella lagen behöver

ändras. Vidare ska regleringen vara helt teknikneutral. Den ska uteslutande bygga på rättsliga gränsdragningar, inte tekniska sådana. Som vi ser det är det bara på det sättet det är möjligt att åstadkomma en reglering som blir hållbar över tid.

Vilka regelverk ska bilda en fungerande helhet?

I våra direktiv framhålls att de grundläggande reglerna i tryckfrihetsförordningen och offentlighets- och sekretesslagen samt den principiella uppbyggnaden av registerförfattningarna bör vara anpassade till varandra för att möjliggöra en ytterligare effektivisering av e-förvaltningen.

Som framgått ovan är en generell utgångspunkt för vårt arbete att myndigheters behandling av personuppgifter inte längre kan betraktas som en separat del av en myndighets verksamhet av det enda skälet att behandlingen är automatiserad. Det innebär att vi i arbetet med att principiellt bygga upp den generella regleringen för att åstadkomma en fungerande helhet tillsammans med andra regelverk inte enbart kan ta hänsyn till att reglerna ska vara anpassade till tryckfrihetsförordningen och offentlighets- och sekretesslagen. De behöver alltså också vara anpassade till de regler som på ett mer allmänt plan styr en myndighets verksamhet. För att åstadkomma en fungerande helhet behöver även t.ex. förvaltningslagen, arkivlagen, myndighetsförordningen m.m. samt andra regelverk och dokument som i olika hänseenden styr myndigheternas verksamhet beaktas. När det övervägs i vilken mån en tänkt generell reglering i ett visst avseende behöver innehålla regler för att ge personuppgifter det skydd som den elektroniska hanteringen ger upphov till, behöver detta alltså ske också mot bakgrund av sådana regler om rättigheter för enskilda och skyldigheter för myndigheter som finns i det förvaltningsrättsliga regelverket i stort.

Att behovet av regler till skydd för personuppgifter på myndighetsområdet övervägs i förhållande till hur myndigheters verksamhet är reglerade i övrigt och de intressen som bär upp sådana regler är helt i överensstämmelse med de grunder som dataskyddsdirektivet bygger på och ger uttryck för. Exempelvis innebär de grundläggande krav som alltid ska iakttas i samband med en viss enskild behandling, krav på lämpliga säkerhetsåtgärder och reglerna om

behandling av känsliga personuppgifter att frågan om en viss behandling är tillåten ska avgöras mot bakgrund av vilken verksamhet det rör och vilka avvägningar mellan olika intressen som behöver göras i den verksamheten och i det konkreta fallet. Vilka resultat sådana avvägningar kan få på myndighetsområdet kommer däremot inte till uttryck i direktivet. Arbetet med att ta fram en generell reglering för myndigheters behandling av personuppgifter innebär emellertid att dataskyddsdirektivets implementering kan konkretiseras och förtydligas på hela myndighetsområdet. Därmed minskar behovet av särskilda registerförfattningar i motsvarande mån.

En ambition med den generella regleringen är alltså att i så hög grad som möjligt fånga upp och formulera regler till skydd för personuppgifter som generellt utgör en ändamålsenlig reglering för myndigheters verksamhet, för att i så stor utsträckning som möjligt minska behovet av särreglering. På så sätt, och genom att den generella regleringen anpassas till samtliga relevanta regelverk på myndighetsområdet, skapas en tydligare och mer lättillämpad helhet när det gäller hantering av personuppgifter på hela myndighetsområdet.

Hur bör förslaget till uppgiftsskyddsförordning beaktas vid utformningen av en generell reglering?

Som redovisats ovan är ett av skälen till utredningens uppdrag att försöka skapa en samlad reglering för myndigheternas behandling av personuppgifter att en sådan kommer att vara mer ändamålsenlig för att möta den förändring som kan antas komma att ske på det unionsrättsliga området genom en förordning som ersätter dataskyddsdirektivet. En samlad reglering kan fungera som ett komplement till eller, vid behov, genomföra delar av den unionsrättsliga regleringen på området.

I skrivande stund pågår arbetet fortfarande med att inom EU förhandla fram förslaget till en uppgiftsskyddsförordning och det går knappast att göra några säkra prognoser om när det arbetet kommer att vara slutfört. Det förefaller mot den bakgrunden inte vara lämpligt att utforma den nya regleringen så att den nu utgör ett komplement till en kommande uppgiftsskyddsförordning. I så fall skulle väsentliga delar av personuppgiftsskyddet som kan förväntas komma att exklusivt regleras i förordningen, exempelvis de grundläggande krav som ska gälla vid all behandling av person-

uppgifter och tillsynsmyndighetens befogenheter, inte kunna regleras i den generella lagen. Ett förslag till en ny reglering skulle i så fall inte kunna innehålla något förslag om en tidpunkt för ikraftträdande, utan den tidpunkten skulle få göras beroende av om och när en uppgiftsskyddsförordning beslutas. Det skulle i sin tur kunna leda till att någon ny generell reglering om myndigheters behandling av personuppgifter inte kan införas förrän i en obestämd framtid. Vad som nu sagts talar för att införandet av en generell reglering inte bör göras beroende av om en uppgiftsskyddsförordning införs.

Vi ser det inte heller som möjligt att nu utforma ett förslag till en reglering som skulle kunna utgöra ett komplement till en kommande uppgiftsskyddsförordning, eftersom förordningens innehåll i skrivande stund inte i alla delar fullt ut kan överblickas, i synnerhet inte på myndighetsområdet. Det kan emellertid redan nu konstateras att förordningen kan antas lämna öppningar för medlemsstaterna att på myndighetsområdet införa en särreglering beträffande frågor som då kan utformas mot bakgrund av nationella regelverk och andra speciella förutsättningar för de egna myndigheternas verksamhet. Om och när en förordning införs kan det därför antas inte behöva göras några genomgripande ändringar i en ny generell reglering. Även denna omständighet talar alltså för att det saknas tillräckliga skäl för att låta införandet av en generell reglering vänta på att en förordning träder i kraft. Tvärtom kommer det nödvändiga anpassningsarbetet att bli betydligt enklare om en sådan reglering redan finns på plats.

Vår ambition vid utformningen av den generella regleringen har därför varit att i stället relatera våra förslag till det som hittills är känt om uppgiftsskyddsförordningens föreslagna innehåll och redovisa ett resonemang om hur en reglering utifrån gällande rätt kan komma att te sig vid ett införande av förordningen. Vi kommer också att i samband med att vi redovisar konsekvenserna av vårt förslag beskriva hur en anpassning av regleringen kan göras då förordningen införs (se avsnitt 19.2).

För att förverkliga en tydligare och mer ändamålsenlig reglering av myndigheters behandling av personuppgifter bör utgångspunkten således vara att den generella regleringen ska kunna träda i kraft så snart som möjligt. Detta talar, menar vi, för att vårt förslag bör ta sikte på att den generella regleringen till form och innehåll ska

förhålla sig till gällande rätt på området, dvs. dataskyddsdirektivet och personuppgiftslagen.

7.2 En generell lag för myndigheters behandling av personuppgifter

7.2.1 En generell reglering bör ha form av lag

Förslag: Den nya generella regleringen bör ha form av lag. Lagen bör heta myndighetsdatalagen.

En generell reglering av vad som ska gälla beträffande myndigheters personuppgiftsbehandling bör ges form av lag. Detta följer redan av att tillämpningsområdet för en sådan reglering bör vara i princip detsamma som förvaltningslagens, dvs. även kommunala förvaltningsmyndigheter bör omfattas liksom myndigheterna under riksdagen. Till detta kommer att lagformen av flera skäl framstår som det naturliga för en reglering av nu aktuellt slag.

Vi redovisar nedan hur vi ser på den lagtekniska utformningen av den generella lagen och hur den förhåller sig till de särregler som kan behövas för vissa myndigheters behandling av personuppgifter. I ett därpå följande avsnitt lämnar vi en utförlig redovisning av vår bedömning när det gäller frågan om på vilken normgivningsnivå en särreglering kan ges, dvs. om särregler kan ges i förordning eller om de behöver ha form av lag.

En allmän utgångspunkt för våra överväganden är, som framgått av avsnitt 7.1, att den generella lagen enbart ska innehålla regler om persondataskydd. Vi föreslår därför att den nya lagen benämns ”myndighetsdatalag”. Namnet är också kort, vilket är ändamålsenligt med tanken på att lagen avses vara tillämplig för i princip alla myndigheter.

Vid personuppgiftslagens införande övervägdes även namnet persondatalag. Skälet till att det namnet inte valdes var bl.a. att det på ett missvisande sätt kunde leda tanken till enbart datorlagrade personuppgifter, trots att lagen inte bara omfattar automatiserad behandling i datorer utan även viss manuell behandling av personuppgifter (prop. 1997/98:44 s. 42). Eftersom myndigheterna i dag i

princip uteslutande hanterar personuppgifter med it-stöd, anser vi att namnet myndighetsdatalag inte gärna kan uppfattas som missvisande.

7.2.2 Kort om lagens innehåll och den lagtekniska utformningen

Vilka frågor bör regleras i lagen?

Vi har ovan redovisat att utgångspunkten för vårt arbete med den generella lagen är att den enbart ska ta sikte på att reglera frågor om det behov av skydd som den automatiserade behandlingen av personuppgifter ger upphov till när myndigheterna hanterar personuppgifter i sin verksamhet. Lagen ska alltså enbart innehålla bestämmelser som utgör dataskyddsregler.

Det innebär att lagen för det första bör innehålla regler som rör frågor där personuppgiftslagens bestämmelser inte på ett tillräckligt tydligt sätt uttrycker vad som gäller för myndigheters behandling av personuppgifter. Det handlar alltså om bestämmelser som särskilt reglerar vad som gäller för myndigheter i en viss fråga till skillnad från vad enskilda personuppgiftsansvariga har att iaktta.

I registerförfattningarna förekommer även bestämmelser som reglerar behandling av personuppgifter utan att de syftar till att införliva dataskyddsdirektivet i något visst avseende. Det är alltså bestämmelser som inte har någon motsvarighet i personuppgiftslagen. Det har ändå ansetts finnas ett behov av att denna typ av bestämmelser för att tydliggöra vad som gäller i förhållande till andra regelverk, framför allt beträffande offentlighets- och sekretesslagens bestämmelser om utbyte av uppgifter i förhållande till både enskilda och andra myndigheter. Som exempel på sådana bestämmelser kan nämnas regler om utlämnande av personuppgifter i elektronisk form, bl.a. genom direktåtkomst. Som har framgått av kapitel 5 menar vi att det finns skäl att upprätthålla den rättsliga skillnaden mellan direktåtkomst och andra former av elektroniskt utlämnande. Bestämmelser rörande detta bör alltså införas även i den generella lagen.

Ett annat exempel på en typ av bestämmelser som vanligen förekommer i registerförfattningar och som inte kan sägas ha sin omedelbara motsvarighet i dataskyddsdirektivet är s.k. sökbegränsningar. Sådana bestämmelser ger emellertid uttryck för den pro-

portionalitetsprincip som alltid måste iakttas när det gäller behandling av personuppgifter och inte minst på myndighetsområdet. Även regler om sökbegränsningar har därför sin plats i en generell lag.

Det kan konstateras att lagen således kommer att få en utformning som i hög grad liknar en författning av den kategori vi benämnt informationshanteringsförfattning, låt vara att denna ”registerförfattning” syftar till att generellt reglera myndigheters behandling av personuppgifter.

Den lagtekniska utformningen

Vi har ovan redovisat vår huvudambition med den generella lagen att i så hög grad som möjligt fånga upp och uttrycka regler till skydd för personuppgifter som generellt utgör en ändamålsenlig reglering för myndigheterna, för att i motsvarande mån minska behovet av särreglering. Det innebär att vi ser framför oss ett relativt begränsat behov av särreglering som kommer att avse förhållandevis få frågor i jämförelse med den regelmassa som i dag finns i registerförfattningarna. Vi bedömer att det därför – på sikt – inte alls kommer att behövas fullständiga registerförfattningar i den utsträckning som är fallet i dag. Författningar som syftar till att reglera regelrätta register, exempelvis fastighetsregistret och aktiebolagsregistret, påverkas dock endast delvis eftersom de typiskt sett syftar till att reglera annat än dataskydd, nämligen verksamhetsfrågor kring ett visst register. Sådana verksamhetsregler utgör ingen särreglering i förhållande till personuppgiftslagen och påverkas därmed inte av den nya lagen. Detta slags registerförfattningar kan alltså inte ersättas av den nya lagen. Inget hindrar dock att dataskyddsregleringen i den nämnda sortens registerförfattning – som efter en översyn fortfarande anses behövas – separeras från författningen och särregleras i anslutning till den nya lagen. Vi återkommer till denna fråga i kapitel 8.

Den generella lagen bör lagtekniskt utformas så att den i sin huvuddel innehåller de bestämmelser som generellt reglerar myndigheternas behandling av personuppgifter i olika avseenden. I en eller flera bilagor till lagen kan därefter tabellvis redovisas sådana särregler för enskilda myndigheter som bör – eller undantagvis behöver

– ges i form av lag. Det kan exempelvis handla om vissa fall av direktåtkomst eller mer tillåtande regler för att behandla känsliga personuppgifter som kan behövas på vissa myndighetsområden och som bedöms kräva lagstöd. Till lagen bör det också finnas en anslutande förordning som innehåller de särregler som kan ges på förordningsnivå. Vi bedömer att den helt övervägande delen av sådan utfyllande reglering kan ges i förordning. I avsnittet nedan redogör vi mer utförligt för vår bedömning av vilken normgivningsnivå som normalt krävs för de särregler som kan behövas.

7.3 Normgivningsnivå för särreglering

7.3.1 Bakgrund

Av 8 kap. 1 § första stycket RF framgår att föreskrifter meddelas av riksdagen genom lag och av regeringen genom förordning. Föreskrifter ska meddelas genom lag om de avser bl.a. skyldigheter för enskilda eller ingrepp i enskildas personliga eller ekonomiska förhållanden (8 kap. 2 § första stycket 2). Kravet på att en sådan föreskrift ska ha form av lag är emellertid inte obligatoriskt, utan riksdagen kan bemyndiga regeringen att meddela den typen av föreskrifter (8 kap. 3 §).

Enligt 8 kap. 7 § RF får regeringen bl.a. meddela föreskrifter som inte enligt grundlag ska meddelas av riksdagen. Att regeringen meddelar föreskrifter i ett visst ämne hindrar inte att riksdagen meddelar föreskrifter i samma ämne (8 kap. 8 §).

Av 8 kap. 10 och 11 §§ RF följer att en vidaredelegation till en förvaltningsmyndighet att meddela föreskrifter också kan medges av riksdagen eller, i fråga om regeringens primärområde, av regeringen själv.

De s.k. registerförfattningarna är ett exempel på en grupp författningar där lagformen ofta valts trots att detta enligt regeringsformen rent normgivningstekniskt i allmänhet inte har varit nödvändigt. Att det allmänna registrerar personuppgifter om enskilda innebär ingen skyldighet för den enskilde. Det har heller normalt sett inte ansetts som ett ingrepp i enskildas personliga förhållanden i den mening som avses i 8 kap. 2 § första stycket 2 RF (Anders Eka m.fl., Regeringsformen – med kommentarer, 2012, s. 311). Registerförfattningarna har därmed i princip ansetts höra till rege-

ringens primärområde – i vart fall såvitt avser myndigheter under regeringen – och således kunnat regleras i förordningsform. Som har berörts tidigare har det under åren emellertid i ett antal olika lagstiftningsärenden som rört myndigheters personuppgiftsbehandling framhållits att målsättningen bör vara att myndighetsregister med ett stort antal registrerade och ett särskilt känsligt innehåll ska regleras i lag (se t.ex. prop. 1997/98:44 s. 41, 1997/98:KU18 s. 43 och prop. 1999/2000:39 s. 78).

Enligt 8 kap. 18 § RF får en lag inte ändras eller upphävas på annat sätt än genom lag. Det är den formella lagkraftens princip som på så sätt kommer till uttryck i regeringsformen. Den formella lagkraftens princip innebär att en föreskrift som en gång beslutats som lag inte kan ändras eller upphävas på annat sätt än genom en ny lag. Regeln om den formella lagkraften får bl.a. den effekten att regeringen inte kan hindra eller upphäva en lag som riksdagen stiftat inom ett område som annars enligt grundlag primärt faller inom regeringens kompetensområde. Inte heller kan regeringen så länge lagen gäller meddela föreskrifter i ämnet i strid med lagen. Riksdagen tar på så vis i anspråk en del av regeringens primärområde. Detta innebär att i den mån myndigheters personuppgiftsbehandling har reglerats genom lag så krävs lagstiftning också för att ändra regleringen.

Enligt 2 kap. 6 § andra stycket RF är var och en gentemot det allmänna skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Av 2 kap. 20 § följer att skyddet mot övervakning och kartläggning av den enskildes personliga förhållanden får begränsas genom lag i den utsträckning det är tillåtet enligt de allmänna förutsättningarna för begränsning av fri- och rättigheter som anges i 21 §. Vid antagande av sådan lag som avses i 20 § är enligt 22 § det s.k. kvalificerade förfarandet tillämpligt. Detta innebär att ett förslag till rättighetsbegränsande lag ska, om det inte avslås av riksdagen, på yrkande av lägst tio av dess ledamöter vila i minst tolv månader från det att det första utskottsyttrandet över förslaget anmäldes i riksdagens kammare.

Motivuttalanden på registerförfattningsområdet rörande normgivningsnivå

De ovan berörda motivuttalandena om att målsättningen bör vara att myndighetsregister med ett stort antal registrerade och ett särskilt känsligt innehåll ska regleras i lag tillkom i samband med det grundlagstiftningsärende där bl.a. Data- och offentlighetskommitténs slutbetänkande behandlades.

Prop. 1990/91:60 innehöll förslag som syftade till att stärka offentlighetsprincipen i fråga om ADB-upptagningar och till att förbättra integritetsskyddet för uppgifter i personregister. Där föreslogs vissa ändringar i tryckfrihetsförordningens bestämmelser om allmänna handlingars offentlighet – bl.a. beträffande den s.k. biblioteksregeln – samt ändringar i sekretesslagstiftningen som innebar preciseringar av det krav på ”god offentlighetsstruktur” som gällde för myndigheternas ADB-verksamhet. Vidare föreslogs bl.a. ändringar i datalagen (1973:289) i syfte att reglera och begränsa användningen av personnummer i personregister. Propositionen behandlades av konstitutionsutskottet i betänkandet 1990/91:KU11.

Vid den aktuella tidpunkten krävdes alltså normalt tillstånd från Datainspektionen för att inrätta och föra särskilt integritetskänsliga ADB-register, dvs. personregister som innehöll ömtåliga uppgifter om enskilda personer. Om inrättandet av ett sådant register beslutades av riksdagen eller regeringen – s.k. statsmaktsregister – räckte det dock med att beslutet föregicks av ett yttrande från Datainspektionen. I debatten hade då och då rests krav på att register av detta slag borde vara lagreglerade, vilket skulle innebära att det skulle krävas ett särskilt riksdagsbeslut för att en myndighet skulle få föra ett personregister som innehöll särskilt integritetskänsliga uppgifter.

I prop. 1990/91:60 gjorde föredragande statsrådet – i likhet med Data- och offentlighetskommittén – bedömningen att som ett led i en allmän strävan att stärka skyddet för de registrerades integritet i samband med nödvändig registrering av känsliga personuppgifter i vissa myndighetsregister på sikt vissa register hos Socialstyrelsen, landstingen, kommunerna och dåvarande Riksförsäkringsverket borde regleras i särskilda registerlagar. Vidare uttalades följande (a. prop. s. 57 f.).

> Som framgått av min redovisning är redan i dag vissa stora personregister med integritetskänsligt innehåll inom den offentliga sektorn författningsreglerade i större eller mindre mån. Flera av de viktigaste

> registren saknar emellertid författningsstöd och några av dem har inte heller tillstånd från datainspektionen eftersom de är undantagna från tillståndsplikt till följd av 2 a § tredje stycket datalagen.
>
> Bland de register som sålunda undantagits från tillståndsplikt kan nämnas personregister som förs av myndigheter inom hälso- och sjukvården för vård- eller behandlingsändamål. I dessa register finns uppgifter om enskildas sjukdomar och hälsotillstånd […]. Vidare kan nämnas de sociala myndigheternas personregister som innehåller uppgifter om att någon fått ekonomisk hjälp eller vård inom socialtjänsten […]. Också dessa personregister har generellt sett ett mycket integritetskänsligt innehåll.
>
> I likhet med [kommittén] och remissinstanserna anser jag att en målsättning bör vara att i de fall ett register med ett stort antal registrerade och ett särskilt känsligt innehåll inrättas, bestämmelser ska meddelas i form av lag. Detta gäller särskilt i de fall uppgifterna i registret sprids externt i icke obetydlig omfattning.
>
> Om uppgifter används för strikt avgränsade ändamål i ett register där de primärt har registrerats, t.ex. inom försvaret eller arbetsmarknadsutbildningen och i många kommunala sammanhang behövs däremot i regel ingen specialreglering. I dessa register kan integritetsskyddet, enligt min mening, tillgodoses genom datainspektionens tillståndsprövning. Om de uppgifter som ingår i registret i sådana fall inte är sekretesskyddade, kan det övervägas om en utvidgning av bestämmelserna i sekretesslagen är en väg att uppnå ett bättre integritetsskydd.

Vidare fördes i propositionen resonemang om behovet av reglering på vissa angivna områden såsom landstingens och kommunernas barnavårds- och skolhälsoregister, Riksförsäkringsverkets och de dåvarande försäkringskassornas register, det s.k. FAS 90 m.fl., samt konstaterades att en reglering var möjlig bara på sikt och att det återstod att närmare överväga vilka register inom de angivna områdena som borde regleras.

Konstitutionsutskottet uttalade som sin mening att det allmänt sett var av stor betydelse att en författningsreglering av ADB-register kommer till stånd i syfte att stärka skyddet för de registrerades integritet i samband med nödvändig registrering av känsliga uppgifter i myndighetsregister. Som anförts i propositionen borde register hos Socialstyrelsen, landstingskommunerna, kommunerna och Riksförsäkringsverket regleras i särskilda registerlagar. Utskottet delade departementschefens uppfattning att det krävdes ingående

överväganden i fråga om vilka register inom dessa områden som borde regleras (1990/91:KU11 s. 11).

I lagstiftningsärendet rörande personuppgiftslagen fördes ett resonemang beträffande registerförfattningarna. Det konstaterades att dessa innehöll många preciserade och viktiga regler som inte rimligen kunde ersättas av de generella bestämmelser som den nya lagen innehöll. Samtidigt stod det klart att det var nödvändigt med särregler i förhållande till den nya lagen på flera viktiga områden, t.ex. beträffande polisens verksamhet. Frågan var därför om det redan i den nya lagen skulle göras undantag för vissa verksamheter eller om nödvändiga särregler för dessa verksamheter liksom dittills skulle ges i särskilda författningar som fick gälla framför den nya lagen.

Regeringen fann att det traditionella svenska systemet med särregler i särskilda författningar var att föredra framför generella undantag från den nya lagen. Eftersom det skulle krävas en särskild författning för att avvika från det integritetsskydd som den nya lagen skulle ge, garanterades att behovet av särregler alltid övervägs noga i den ordning som gäller för författningsgivning. Vidare uttalades – med hänvisning till de uttalanden som gjorts i 1991 års grundlagsstiftningsärende (prop. 1990/91:60 s. 50 och 1990/91:KU11 s. 11) – att målet också har varit att myndighetsregister med ett stort antal registrerade och ett särskilt känsligt innehåll ska regleras särskilt i lag. Det fanns inte anledning att nu avvika från det målet (prop. 1997/98:44 s. 41).

I konstitutionsutskottets betänkande rörande personuppgiftslagen påpekades med anledning av en motion att i den utsträckning som det är befogat med ett ställningstagande från riksdagens sida, finns det alltid möjlighet att ge regleringen på ett visst område i lag. I sådant fall är normgivning på lägre nivå i strid med lagregleringen utesluten, om inte annat följer av den aktuella lagen. Utskottet ville också för egen del framhålla att det saknades anledning att nu avvika från den tidigare fastlagda målsättningen att myndighetsregister med att stort antal registrerade och ett särskilt känsligt innehåll ska regleras särskilt i lag (1997/98:KU18 s. 43).

De uttalanden som gjordes beträffande behovet av lagform vid 1991 års grundlagsstiftningsärende och som bekräftades i samband med införandet av personuppgiftslagen har alltså under åren åberopats i ett stort antal lagstiftningsärenden i samband med överväganden kring frågan varför en viss registerförfattning borde ges

lagform (se t.ex. prop. 1999/2000:39 s. 78, prop. 2000/01:80 s. 131, prop. 2000/01:95 s. 55 och prop. 2002/03:135 s. 39).

Den tidigare grundlagsregleringen beträffande skyddet för den personliga integriteten

Under 1980-talet inträffade en rad händelser som väckte misstro mot den då ännu förhållandevis nya datatekniken och det sätt på vilket staten använde sig av denna för att registrera medborgarna. Exempelvis orsakade planer på en ny typ av folk- och bostadsräkning, benämnt Fobalt, byggd på samkörning av redan befintliga register, så häftiga protester att projektet inte kunde genomföras. År 1986 avslöjades att det sociologiska forskningsprojektet Metropolit med Datainspektionens medgivande under lång tid hade samlat in och registrerat stora mängder känsliga persondata avseende cirka 15 000 utvalda svenskar och deras familjer. Avslöjandet ledde till ytterst skarp kritik i medierna och fick också politiska återverkningar.

Den år 1984 tillkallade Data- och offentlighetskommittén sökte fånga upp den utbredda oro för myndigheternas registerutnyttjande som fanns vid denna tid genom att i delbetänkandet Integritetsskyddet i informationssamhället 3, Grundlagsfrågor (Ds Ju 1987:8) föreslå en ny regel i regeringsformens fri- och rättighetskapitel av innebörd att varje medborgare skulle vara ”tillförsäkrad skydd mot registrering av uppgifter om honom med hjälp av automatisk databehandling enligt bestämmelser som meddelas i lag”. Av delbetänkandet framgår att kommittén var väl medveten om att ett sådant lagstadgat skydd redan fanns, främst genom datalagen och sekretesslagen, och att det föreslagna stadgandet i regeringsformen därför inte syftade till att stärka det materiella skyddet för den personliga integriteten utan i stället borde ses som en markering av vilken vikt samhället tillmätte själva frågan. Regeringen instämde i allt väsentligt i Data- och offentlighetskommitténs bedömningar. Föredragande statsrådet anförde att regeringens utgångspunkt var att ”ge grundlagsförankring åt det skydd för medborgarna som redan finns genom vanlig lagstiftning och på detta sätt befästa det rådande rättsläget”. Den reella innebörden var enligt förarbetena att riksdagen måste vara aktiv genom att stifta och vidmakthålla en datalagstiftning (prop. 1987/88:57 s. 9 och 11).

Lagförslaget antogs av riksdagen och innebar att, med ikraftträdande den 1 januari 1989, ett nytt andra stycke infördes i 2 kap. 3 § RF med följande lydelse.

> Varje medborgare skall i den utsträckning som närmare angives i lag skyddas mot att hans personliga integritet kränkes genom att uppgifter om honom registreras med hjälp av automatisk databehandling.

Bestämmelsen kom att gälla oförändrad fram till den 1 januari 2011.

År 1994 infördes i regeringsformen (dåvarande 8 kap. 7 §) en möjlighet för riksdagen att till regeringen eller den myndighet som regeringen bestämmer delegera rätten att meddela föreskrifter om skydd för personlig integritet vid registrering av uppgifter med hjälp av automatisk databehandling, varvid regeln i 2 kap. 3 § andra stycket inte ansågs hindra sådan delegation (prop. 1993/94:116 s. 15). I samband med införandet av personuppgiftslagen ändrades delegationsbestämmelsen i 8 kap. RF. Däremot gjordes alltså inga ändringar i 2 kap. 3 §.

Den nu gällande regleringen

Våren 2004 tillkallades en parlamentariskt sammansatt kommitté – Integritetsskyddskommittén – som bl.a. fick i uppgift att kartlägga och analysera sådan lagstiftning som rör den personliga integriteten, överväga om regeringsformens bestämmelse om skyddet för den personliga integriteten i dåvarande 2 kap. 3 § andra stycket RF borde ändras och i så fall föreslå en ny grundlagsreglering.

I januari 2008 överlämnade Integritetsskyddskommittén sitt slutbetänkande SOU 2008:3. I betänkandet uttalades bl.a. att kommitténs kartläggning och analys hade visat att lagstiftaren inte lägger tillräcklig vikt vid integritetsskyddsaspekter när ny lagstiftning arbetas fram. Även rent allmänt värderades integritetsskyddet förhållandevis lågt i lagstiftningen. En bidragande orsak till detta fick anses vara att det i grundlagen inte fanns någon rättsligt verkande bestämmelse om medborgarnas rätt till skydd för personlig integritet som balanserar de övriga fri- och rättigheter som medborgarna är tillförsäkrade. Enligt kommittén var det sammanfattningsvis tydligt att det på grundlagsnivå behövde ges uttryck för en större respekt än för närvarande för den enskildes rätt till personlig integritet. Bestämmelser som ger ett utvidgat materiellt integritets-

skydd borde därför införas i regeringsformens kapitel om grundläggande fri- och rättigheter (SOU 2008:3 s. 255 f.).

Integritetsskyddskommittén föreslog att ett nytt andra stycke av följande lydelse skulle införas i 2 kap. 6 §:

> Även i annat fall än som avses i första stycket är varje medborgare gentemot det allmänna skyddad mot intrång, om det sker i hemlighet eller utan samtycke och i betydande mån innebär övervakning eller kartläggning av den enskildes personliga förhållanden.

Beträffande den föreslagna bestämmelsens tillämpning på hantering av personuppgifter i omfattande informationssamlingar gjorde kommittén följande uttalanden (a. a. s. 271).

> Det allmännas hantering av uppgifter om enskilds personliga förhållanden sker inte sällan utan samtycke från den enskilde och kan till och med ske i hemlighet. Sådan hantering kan ha som uttalat syfte att kartlägga den enskildes personliga förhållanden. Som exempel på en hantering som rör uppgifter om enskilda personer som både sker i hemlighet och innebär en kartläggning av den enskildes personliga förhållanden av sådan omfattning att den bör omfattas av det nya grundlagsskyddet kan nämnas Säkerhetspolisens hantering av personuppgifter. Som ett annat exempel kan nämnas polisens personuppgiftshantering i underrättelseverksamhet och under en brottsutredning.
>
> […]
>
> Som exempel på myndigheter eller myndighetsområden som har informationssamlingar beträffande enskildas personliga förhållanden som kan sägas ha en sådan omfattning att de i praktiken innebär en kartläggning, och i hög utsträckning består av uppgifter som ansetts särskilt skyddsvärda, kan nämnas Skatteverket, Kronofogdemyndigheten, Försäkringskassan och socialtjänsten. En personuppgiftshantering som uteslutande sker av administrativa skäl, vilken regelmässigt brukar omfattas av svag eller ingen sekretess, kan däremot inte anses ha ett sådant skyddsvärde att den bör omfattas av ett grundlagsskydd för den personliga integriteten.
>
> När det gäller hantering av personuppgifter i de informationssamlingar som kommer att omfattas av det utvidgade grundlagsskyddet är det självfallet så att inte alla led i hanteringen är att betrakta som sådana intrång som behöver omfattas av de särskilda förutsättningar som gäller för att intrång i den grundlagsskyddade rättigheten skall vara tillåtet. De från integritetsskyddssynpunkt viktigaste momenten i hanteringen handlar om hur uppgifter om enskilda får samlas in, ändamålet med behandlingen och i vilken utsträckning uppgifter på grund av uppgiftsskyldighet, som alltså bryter sekretess som gäller för

uppgifterna, skall lämnas ut till andra för samkörning med uppgifter i andra myndighetsregister eller av andra skäl.

2010 års ändringar av regeringsformen

I prop. 2009/10:80 lade regeringen fram förslag till omfattande ändringar av regeringsformen som väsentligen byggde på Grundlagsutredningens förslag. I samma lagstiftningsärende föreslog regeringen en ny bestämmelse i 2 kap. RF som väsentligen byggde på Integritetsskyddskommitténs förslag. Förslaget antogs av riksdagen och den nya bestämmelsen i 2 kap. 6 § andra stycket RF trädde – liksom övriga grundlagsändringar – i kraft den 1 januari 2011.

Den nya bestämmelsen är utformad så att den reglerar förhållandet mellan den enskilde och det allmänna och sägs utgöra en begränsning av statsmakternas normgivningsbefogenheter inom ramen för rättighetsskyddet (prop. 2009/10:80 s. 176). Den är alltså avsedd att få sin huvudsakliga innebörd genom de begränsningar som gäller för riksdagen att inskränka fri- och rättigheter (20–22 §§). Det finns däremot inte några sådana särskilda begränsningsförutsättningar som finns för bl.a. begränsningar av yttrande- och informationsfriheten (jfr 2 kap. 23 och 24 §§).

Bestämmelsen innebär enligt sin ordalydelse att enskilda är skyddade mot åtgärder från det allmännas sida som innefattar betydande intrång i den personliga integriteten, om intrånget sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. I motiven förs resonemang om hur dessa olika kriterier är avsedda att förstås (prop. 2009/10:80 s. 177 f.).

Uttrycket ”personliga förhållanden” avses ha samma innebörd som i tryckfrihetsförordningen och offentlighets- och sekretesslagen (2009:400). Det innebär att regleringen kan komma att omfatta vitt skilda slag av information som är knuten till den enskildes person, t.ex. uppgifter om namn och andra personliga identifikationsuppgifter, adress, familjeförhållanden, hälsa och vandel. Även fotografisk bild samt uppgifter som inte är direkt knutna till den enskildes privata sfär, t.ex. uppgift om anställning, omfattas av uttrycket. Liksom vid tillämpningen av offentlighets- och sekretesslagstiftningen får vid prövningen av uttryckets närmare innebörd

vägledning hämtas från vad som enligt normalt språkbruk kan läggas i dess betydelse.

Vid behandlingen av uppgifter som rör den enskilde får ett integritetsintrång normalt anses större om behandlingen sker utan den enskildes samtycke än om det sker efter dennes medgivande. Innebörden av kravet på samtycke bör enligt motiven bedömas på samma sätt som motsvarande krav enligt bestämmelsen om förbud mot åsiktsregistrering i regeringsformen (2 kap. 3 §). Avgörande för om en åtgärd ska anses innebära övervakning eller kartläggning är inte dess huvudsakliga syfte utan vilken effekt åtgärden har. Vad som avses med övervakning respektive kartläggning får bedömas med utgångspunkt från vad som enligt normalt språkbruk läggs i dessa begrepp (prop. 2009/10:80 s. 250). Beträffande ”kartläggning” görs i motiven vidare följande uttalande (a. prop. s. 180).

> En åtgärd från det allmännas sida som vidtas primärt i syfte att ge myndigheterna underlag för beslutsfattande i enskilda fall, exempelvis insamling av uppgifter av visst slag för beslut om t.ex. beskattning eller liknande, kan – även om avsikten inte är att kartlägga enskilda – i många fall anses innebära kartläggning av enskildas förhållanden. Så torde fallet vara i fråga om ett stort antal uppgiftssamlingar som det allmänna förfogar över. En mycket stor mängd information som rör enskildas personliga förhållanden finns t.ex. lagrad i Skatteverkets, Tullverkets, Försäkringskassans och Kronofogdemyndighetens olika databaser. Även Statistiska centralbyrån och andra statistikansvariga myndigheter, t.ex. Socialstyrelsen och Brottsförebyggande rådet, lagrar och bearbetar stora mängder uppgifter om enskildas personliga förhållanden i sina databaser. Flera av dessa uppgiftssamlingar omfattar en stor andel av landets hela befolkning och flera av dem innehåller också till viss del mycket integritetskänsliga uppgifter. Myndighetsspecifika verksamhetsregister och databaser med information som är knuten till en myndighets ärendehantering förekommer inom i stort sett all statlig och kommunal förvaltning. Särskilda föreskrifter som anger de närmare förutsättningarna för informationshanteringen finns för t.ex. socialtjänsten, studiestödsverksamheten, Kriminalvården och den brottsbekämpande verksamheten hos såväl polismyndigheterna, Tullverket och åklagarmyndigheterna som Skatteverket och Kustbevakningen samt hos domstolarna. I flertalet fall är uppgifterna tillgängliga för myndigheterna på sådant sätt att lagringen och behandlingen av uppgifterna kan sägas innebära att enskilda kartläggs, även om det huvudsakliga ändamålet med behandlingen är ett helt annat. Det förekommer även att uppgiftssamlingar inrättas och utformas i syfte att fungera som mer utpräglade personregister. Som exempel kan nämnas polisens belastningsregister. Registreringen av personuppgifter i registret kan sägas innebära en kartläggning av alla dem som har

dömts eller på annat sätt lagförts för brott, även om registrets uttalade ändamål är att ge information åt olika myndigheter om belastningsuppgifter som behövs bl.a. för att utreda brott och bestämma straff samt vid lämplighets- och tillståndsprövning av skilda slag. På liknande sätt förhåller det sig med många andra register som används i den brottsbekämpande verksamheten, t.ex. polisens misstankeregister, fingeravtrycks- och DNA-register m.m. I detta sammanhang kan även nämnas de olika associationsrättsliga register som Bolagsverket ansvarar för, bl.a. aktiebolagsregistret, handelsregistret och föreningsregistret. En omfattande behandling av personuppgifter sker vidare inom t.ex. hälso- och sjukvården.

Vid bedömning av vilka åtgärder som kan anses utgöra ett ”betydande intrång” ska enligt motiven både åtgärdens omfattning och arten av det intrång åtgärden innebär beaktas. Även åtgärdens ändamål och andra omständigheter kan ha betydelse.

Några exempel på tillämpningen

Datalagringsdirektivet

I prop. 2010/11:46 lämnades förslag till genomförande av Europaparlamentets och rådets direktiv 2006/24/EG om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/58/EG. Direktivet syftade till att harmonisera medlemsstaternas regler om skyldigheter för leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät att lagra trafik- och lokaliseringsuppgifter samt uppgifter som behövs för att identifiera en abonnent eller användare för att säkerställa att uppgifterna finns tillgängliga för avslöjande, utredning och åtal av allvarliga brott.

Direktivet föreslogs bli genomfört i svensk rätt genom regler intagna i lagen (2003:389) om elektronisk kommunikation, LEK. Lagringsskyldig skulle enligt 6 kap. 16 a § LEK den vara som bedriver anmälningspliktig verksamhet enligt 2 kap. 1 § samma lag. Därigenom omfattas leverantörer av allmänt tillgängliga kommunikationsnät.

I yttrande till justitieutskottet gjorde konstitutionsutskottet bedömningen att det var fråga om mycket omfattande informations-

samlingar som delvis avser integritetskänsliga uppgifter, nämligen om vem som kommunicerade med vem, när det skedde, var de som kommunicerade befann sig och vilken typ av kommunikation som användes. Enligt utskottets mening sker ett integritetsintrång redan genom att uppgifterna lagras, även om merparten av de uppgifter som föreslås ska lagras troligen aldrig kommer att begäras ut för brottsutredningar. I likhet med regeringen ansåg därför utskottet att lagringen av trafikuppgifter medför ett intrång i enskildas personliga integritet. Intrånget måste, mot bakgrund av den mängd trafikuppgifter om en enskild som kan komma att lagras, anses vara betydande. Den lagring av trafikuppgifter som föreslogs i propositionen omfattades därför enligt utskottets mening av regeringsformens skydd i 2 kap. 6 § andra stycket för den personliga integriteten (2010/11:JuU14).

Det aktuella lagförslaget förklarades i mars 2011 vilande enligt 2 kap. 22 § RF. I mars 2012 avgav justitieutskottet i enlighet med dåvarande 4 kap. 9 § RO ett nytt betänkande i ärendet (2011/12:JuU28). Utskottet fann vid sin förnyade beredning av ärendet inte skäl att frångå den bedömning som gjordes i betänkande 2010/11:JuU14. Lagändringarna trädde i kraft den 1 maj 2012 (SFS 2012:126 och 127).

Den 8 april 2014 meddelade EU-domstolen dom i de förenade målen C-293/12 och C594/12, Digital Rights Ireland m.fl. I domen förklarade EU-domstolen datalagringsdirektivet ogiltigt. I Ds 2014:23 har gjorts en analys av vad domen får för konsekvenser för svensk rätt.

Kustbevakningsdatalagen

I prop. 2011/12:45 lade regeringen fram förslag till en lag om behandling av personuppgifter i Kustbevakningens verksamhet, en kustbevakningsdatalag. Syftet med den föreslagna lagen var att ge Kustbevakningen möjlighet att behandla personuppgifter på ett effektivt och ändamålsenligt sätt i sin verksamhet och att skydda människor mot att deras personliga integritet kränks vid sådan behandling. Den föreslagna lagen reglerar, med några få undantag, all behandling av personuppgifter i Kustbevakningens operativa

verksamhet. Lagen ersatte förordningen (2003:188) om behandling av personuppgifter inom kustbevakningen.

Kustbevakningens verksamhet kan, något förenklat, delas in under de två huvudrubrikerna sjöövervakning och räddningstjänst. Kustbevakningens uppgifter regleras primärt i förordningen (2007:853) med instruktion för Kustbevakningen, men även i de särskilda lagar och förordningar som innehåller bestämmelser om verksamheten samt i regleringsbrev och enskilda regeringsbeslut. Nämnas kan t.ex. lagen (1982:395) om Kustbevakningens medverkan vid polisiär övervakning, lagen (2000:1225) om straff för smuggling, narkotikastrafflagen (1968:64), sjölagen (1994:1009), lagen (2003:778) om skydd mot olyckor och fartygssäkerhetslagen (2003:364).

Beträffande behovet av en ny lagstiftning rörande Kustbevakningens personuppgiftsbehandling gjordes bl.a. följande uttalande (prop. 2011/12:45 s. 62).

> Personuppgiftslagen gäller generellt för all behandling av personuppgifter, såvida det inte finns avvikande regler i lag eller förordning. I det lagstiftningsärende som föregick personuppgiftslagen uttalade regeringen att lagen i princip bara bör innehålla generella regler och att behovet av undantag och särregler för mer speciella områden får tillgodoses genom andra författningar (prop. 1997/98:44 s. 40 f.). Sådan författningsreglering, främst i form av s.k. registerlagar, har skett utifrån det principiella ställningstagandet att myndighetsregister med ett stort antal registrerade personer och ett integritetskänsligt innehåll bör regleras i lag.
>
> Sedan den 1 januari 2011 är enskilda skyddade gentemot det allmänna mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär kartläggning eller övervakning av personliga förhållanden (2 kap. 6 § RF). Inskränkningar i detta skydd kan enbart ske i lag och bara för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle (2 kap. 20 och 21 §§ RF). Utgångspunkten för behovet av och villkoren för lagregleringen av behandling av personuppgifter som utförs av myndigheter bör således numera tas i regeringsformens bestämmelser om integritetsskydd. Med hänsyn till omfattningen och arten av Kustbevakningens verksamhet, den ingripande myndighetsutövning som ingår i uppgiften samt behovet av att kunna behandla personuppgifter även av känsligare slag inom främst den brottsbekämpande verksamheten anser regeringen att stora delar av Kustbevakningens personuppgiftsbehandling innefattar sådan integritetskänslig informationshantering som enskilda är skyddade mot enligt 2 kap. 6 § andra stycket RF. Det finns därför ett behov av en särskild författningsreglering i lag av behandlingen av personuppgifter i Kustbevakningens verksamhet.

Uppgiftsutlämnande till utlandet m.m.

I prop. 2010/11:129 lämnades förslag på de lagändringar som krävdes för att genomföra det automatiserade utbyte av DNA-profiler, fingeravtryck och fordonsuppgifter som föreskrivs i EU:s rådsbeslut om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och annan gränsöverskridande brottslighet, det s.k. Prümrådsbeslutet.

Medlemsstaterna ska enligt rådsbeslutet ge varandra tillgång till uppgifter i de nationella DNA-, fingeravtrycks- och fordonsregistren. Uppgifterna ska utbytas via nationella kontaktställen som ska kunna göra automatiska sökningar i övriga medlemsstaters register.

Mot bakgrund av 2 kap. 6 § andra stycket RF gjordes i propositionen den bedömningen att utländska myndigheters direktåtkomst till svenska register och svenska myndigheters direktåtkomst till utländska register bör regleras i lag (prop. 2010/11:129 s. 49 f).

Beträffande frågan om hur utbyte av uppgifter ur kriminalregister mellan EU:s medlemsstater i olika hänseenden förhåller sig till kravet på lagform enligt 2 kap. 6 § andra stycket RF, se prop. 2011/12:163 s. 26 f.

7.3.2 Våra överväganden

Bedömning: Det torde höra till undantagen att en behandling av personuppgifter sedd för sig kan anses utgöra ett ingrepp i enskildas personliga förhållanden och därför kräver stöd i lag enligt 8 kap. 2 § första stycket 2 RF för att vara tillåten. Från normgivningssynpunkt saknas det därför som huvudregel hinder mot att bestämmelser som avviker från eller kompletterar innehållet i den generella lagen i form av t.ex. myndighetsspecifika föreskrifter om sökbegränsningar, direktåtkomst, behandling av känsliga personuppgifter m.m. ges i förordningsform.

I den mån sådana myndighetsspecifika föreskrifter av något skäl ändå bedöms utgöra ingrepp i enskilds personliga förhållanden och därför kräver lagform kan de tas in i bilaga till den generella lagen eller i annan lag.

Bortsett från de brottsbekämpande myndigheterna torde det bara vara i rena undantagsfall som behandling av personuppgifter

hos myndigheter kan anses innehålla några sådana särskilda moment som är av det slaget att behandlingen måste ha stöd i en sådan lag som endast får beslutas enligt reglerna i 2 kap. RF.

Den nya grundlagsbestämmelsen med ett kompletterande skydd för den personliga integriteten i 2 kap. 6 § andra stycket RF omfattar ett skydd mot betydande intrång. En fråga i detta sammanhang är därför vad som över huvud taget är att betrakta som intrång i den personliga integriteten när det gäller automatiserad behandling av personuppgifter. Den frågan har inte behandlats närmare i förarbetena till bestämmelsen. Bestämmelsen tar inte heller sikte specifikt på sådan behandling, utan i allmän mening användning av information som rör vars och ens personliga förhållanden. I förarbetena anförs att grundlagsbestämmelsen är tillämplig när det är frågan om ett betydande ingrepp i den enskildes privata sfär (prop. 2009/10:80 s. 250). Vi har alltså anledning att inledningsvis ställa oss frågan när en automatiserad behandling alls kan utgöra ett ingrepp i den enskildes privata sfär. Först därefter kan ställning tas till när en behandling av personuppgifter också är att anse som ett betydande ingrepp.

Utgångspunkten i flera av de internationella konventioner och andra dokument som Sverige har förbundit sig att följa på dataskyddets område är att den enskildes rätt till sin personliga integritet kan behöva skyddas i förhållande till principen om ett fritt flöde av information, oberoende av gränser, som också finns inskriven i många internationella överenskommelser om fri- och rättigheter. Så är exempelvis fallet med Europarådets konvention om skydd för enskilda vid automatisk databehandling (CETS 108) och dataskyddsdirektivet.

För svenskt vidkommande är utgångspunkten i normgivningshänseende – i vart fall såvitt avser myndigheter under regeringen – att det förhållandet att det allmänna registrerar personuppgifter om enskilda inte innebär några skyldigheter för den enskilde och inte heller i övrigt avser ingrepp i enskildas personliga förhållanden i den mening som avses i 8 kap. 2 § första stycket 2 RF. Bestämmelser om behandling av personuppgifter är i stället i princip att anse som bestämmelser som införs för att skydda den enskilde. Registerförfattningar som reglerar behandling av personuppgifter hos de statliga myndigheter som lyder under regeringen anses

därför i princip kunna ha form av förordning enligt 8 kap. 7 § första stycket 2, dvs. de hör till regeringens primärområde.

Föreskrifter om behandling av personuppgifter anses alltså i princip ha till effekt att skydda den enskilde från en annars fri användning av uppgifterna. Frågan om när en automatiserad behandling av personuppgifter kan utgöra ett intrång i den enskildes personliga integritet kan emellertid inte besvaras så enkelt som att så är fallet om behandlingen strider mot meddelade dataskyddsbestämmelser. Även bestämmelser som tillåter en viss behandling kan i princip innebära ett intrång i den enskildes personliga integritet. Det hör samman med att varken vars och ens rätt till respekt för sitt privat- och familjeliv enligt artikel 8 i Europakonventionen eller den mer begränsade rätten till grundlagsskydd för den personliga integriteten i 2 kap. RF utgör några absoluta rättigheter. De är i stället att betrakta som s.k. relativa rättigheter, eftersom de kan inskränkas i de fall och på det sätt som anges i respektive regelverk. Man måste alltså skilja på tillåtna och otillåtna intrång i den enskildes personliga integritet.

Av Europadomstolens praxis rörande artikel 8 kan läsas ut att behandling av personuppgifter som är av känslig art i många fall kan anses beröra rätten till respekt för privatlivet. Beroende på omständigheterna kan artikeln anses ställa krav på behandlingen av sådana uppgifter i tre avseenden; dels i fråga om det berättigade i att alls registrera dem, dels i fråga om rätt för den enskilde att själv få ta del av uppgifterna och dels slutligen i fråga om skydd mot att andra får tillgång till uppgifterna (SOU 2008:3 s. 78 f.). I sina avgöranden har domstolen först tagit ställning till om behandlingen av personuppgifter i sig har utgjort ett intrång i den enskildes privatliv. Om ett intrång föreligger, har domstolen därefter bedömt om intrånget har haft ett legitimt intresse och i övrigt uppfyllt förutsättningarna för att intrånget ska anses förenligt med konventionen. Först om det har varit frågan om ett intrång som inte uppfyller konventionens krav har intrånget varit att anse som ett brott mot konventionen, varmed den enskilde har rätt till kompensation för kränkningen (se t.ex. målet Segerstedt-Wiberg m.fl. mot Sverige, dom den 6 juni 2006).

Europakonventionen utgör sedan år 1995 svensk lag. Rättigheterna i konventionen har vidare bekräftats i EU:s rättighetsstadga, som gjorts bindande för medlemsstaterna genom att en hänvisning till

stadgan har införts i artikel 6.1 i EU-fördraget. I rättighetsstadgan anges i artikel 7 att var och en har rätt till respekt för sitt privatliv och familjeliv, sin bostad och sina kommunikationer. Vidare föreskrivs i artikel 8 att var och en har rätt till skydd för de personuppgifter som rör honom eller henne. Dessa uppgifter ska behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim eller lagenlig grund. Var och en har rätt att få tillgång till insamlade uppgifter som rör honom eller henne och att få rättelse av dem. I artikeln anges också att en oberoende tillsynsmyndighet ska se till att dessa regler efterlevs.

Sett i perspektivet av den enskildes numera lagstadgade rätt till skydd för sitt privatliv i samband med behandling av personuppgifter kan en bestämmelse som exempelvis tillåter det allmänna att utan samtycke från den enskilde behandla känsliga personuppgifter utgöra ett intrång i den enskildes personliga integritet. En sådan bestämmelse är alltså inte någon skyddsbestämmelse, utan skyddet i det fallet ligger i rättighetsbestämmelsen. En helt annan sak är att det ändå kan vara frågan om ett tillåtet intrång, om det uppfyller Europakonventionens krav på legitimitet och proportionalitet. Samma resonemang torde exempelvis kunna föras i fråga om dataskyddsdirektivets möjlighet för medlemsstaterna att besluta om undantag från förbudet mot att utan samtycke behandla känsliga personuppgifter om det finns ett viktigt allmänt intresse. Om ett undantag beslutas, torde det alltså i och för sig utgöra ett intrång i den enskildes rätt till en privat sfär, men det kan vara ett tillåtet intrång. I detta fall är det alltså bestämmelsen i direktivet – införlivad i den nationella lagstiftningen – som utgör skyddsbestämmelsen, medan den bestämmelse som medger ett undantag med hänsyn till ett viktigt allmänt intresse är att se som ett intrång i den enskildes rätt.

En föreskrift som tillåter ett intrång i den enskildes rätt till personlig integritet, exempelvis genom att känsliga personuppgifter får behandlas utan samtycke, är rimligen också att se som ett ingrepp i enskilds personliga förhållanden. Det följer därmed av 8 kap. 2 § första stycket 2 RF att en sådan föreskrift ska ha form av lag eller i vart fall stöd av lag (jfr 8 kap. 3 § RF).

När registerlagar beslutas har det i allmänhet inte diskuterats i förarbetena huruvida lagnivån har betingats av att regleringen inte bara innehåller renodlade skyddsbestämmelser, som i och för sig

skulle kunna meddelas i form av en förordning, utan för att den också innehåller bestämmelser som tillåter ett ingrepp i den enskildes personliga förhållanden. Vanligt är i stället att den ovan redovisade motivledes uttalade ambitionen från tidigt 1990-tal åberopas, som innebär att myndighetsregister med ett stort antal registrerade och ett särskilt känsligt innehåll ska regleras i lag. Denna uttalade ambition har med åren kommit att appliceras inte bara på förandet av regelrätta register, utan i vissa fall också på myndigheters personuppgiftsbehandling som sådan. Om behandlingen t.ex. har innefattat stora mängder uppgifter eller särskilt känsliga uppgifter har det ofta ansetts föreligga ett behov av lagstöd även utan någon koppling till företeelsen ”register”. Något klart uttalande om huruvida det finns moment i författningen som innebär att det enligt 8 kap. RF krävs lagstöd eller om det snarare är frågan om en politisk ambition att skyddsregler i dessa fall bör finnas på denna nivå har således i allmänhet inte lämnats. Efter personuppgiftslagens införande har det inte heller förts några resonemang om huruvida den lagen skulle kunna anses utgöra ett tillräckligt lagstöd.

Som exempel på de resonemang i normgivningsfrågan som brukar föras i lagstiftningsärenden om nya registerförfattningar kan nämnas att Lagrådet i samband med införandet av registerförfattningar för Skatteverket, Kronofogdemyndigheten och Tullverket uttalade att svensk rätt i och för sig inte fordrar att föreskrifter av det slag som fanns i de föreslagna lagarna ges form av lag. Det medförde att de normgivningsbemyndiganden som kunde finnas i förslagen i princip var onödiga (prop. 2000/01:33 s. 345). Regeringen kommenterade inte Lagrådets uttalande på annat sätt än att bestämmelser i de olika lagarna om att regeringen meddelar närmare föreskrifter hade utformats i enlighet med Lagrådets synpunkter (se t.ex. a. prop. s. 202). Det innebär emellertid att regeringen i och för sig får anses ha instämt i bedömningen att bestämmelserna inte till någon del omfattades av ett krav enligt 8 kap. RF på att välja lagformen för de aktuella författningarna, men att den formen ändå valdes (jfr a. prop. s. 121). När nya registerförfattningar införs handlar resonemangen kring normnivå också vanligtvis om vad författningen som sådan anses kräva, i stället för vilka enskilda föreskrifter som eventuellt ska meddelas i form av lag.

Att resonemangen om normnivå för registerförfattningar har en politisk snarare än en rättslig prägel torde ha sin bakgrund i att de

första uttalandena om denna politiska ambition gjordes vid en tid då skyddet för den enskildes integritet hade fått en ökad aktualitet genom en allmän debatt där myndigheternas användning av personuppgifter i vissa register kritiserades. Då fanns emellertid ännu inte någon rättsligt bindande regel som innebar ett allmänt skydd för personlig integritet i svensk lagstiftning, eftersom Europakonventionen ännu inte var inkorporerad. Det som fanns i form av en generell regel var målsättningsstadgandet i 1 kap. 2 § fjärde stycket RF som föreskriver att det allmänna ska verka för att demokratins idéer blir vägledande inom samhällets alla områden samt värna den enskildes privatliv och familjeliv.

Den nya bestämmelsen i 2 kap. 6 § andra stycket RF om ett generellt, om än begränsat, skydd för den personliga integriteten syftar alltså inte till att ange vilka föreskrifter om exempelvis behandling av personuppgifter som ska ha form av lag i stället för förordning. Snarare torde bestämmelsen, som vi ser det, såvitt avser behandling av personuppgifter primärt ha funktionen att bland sådana intrång som omfattas av lagkravet enligt 8 kap. 2 § första stycket 2 RF skilja ut de intrång som är så kvalificerade att de ska omfattas av de särskilda begränsningar som enligt 2 kap. 20–22 §§ gäller för riksdagens möjligheter att besluta om en rättighetsinskränkande lag. Samtidigt följer det av regleringen rörande ikraftträdandet av 2 kap. 6 andra stycket RF – äldre föreskrifter som ger stöd för åtgärder som innebär betydande intrång i den personliga integriteten behåller under en övergångsperiod sin giltighet även om föreskrifterna inte uppfyller regeringsformens krav på lagform – att lagstiftaren har utgått från att det kan finnas regler som omfattas av bestämmelsen utan att för den skull också omfattas av något lagkrav enligt 8 kap. RF.

Utgångspunkten är emellertid att integritetsintressen som faller utanför grundlagsbestämmelsens tillämpningsområde, exempelvis vid behandling av personuppgifter, alltså inte behöver sakna skydd utan att där ändå kan gälla ett krav på att ett intrång tillåts enbart i form av lag (jfr prop. 2009/10:80 s. 177). Utrymmet för åtgärder som innebär begränsningar i den enskildes rätt till respekt för privatlivet begränsas vidare genom de krav som följer av Europakonventionen.

Vad får den höga detaljeringsgraden på lagnivå för konsekvenser?

Det kan visserligen hävdas att den uttalade ambitionen att myndighetsregister med ett stort antal registrerade och ett särskilt känsligt innehåll ska regleras i lag i principiell mening har varit en god sak från integritetsskyddssynpunkt. Emellertid torde det enbart vara ett fåtal föreskrifter om myndigheters behandling av personuppgifter som i rättslig mening kräver lagstöd. I stället torde merparten kunna meddelas i form av förordning. Vi återkommer till denna fråga nedan.

Ambitionen att ha samtliga de föreskrifter som behövs för ett visst verksamhetsområde eller en viss myndighets behandling av personuppgifter i en särskild författning på lagnivå har emellertid medfört uppenbara olägenheter för utvecklingen av en effektiv förvaltning eftersom det har inneburit en onödigt hög detaljeringsgrad på lagnivå. Reformarbeten som syftar till att effektivisera myndigheternas hantering av sina ärenden, att ge en förbättrad service när det gäller enskildas insyn allmänt och i egna ärenden och att samverka med myndigheter och andra aktörer, och som inte i något avseende innebär ett intrång i de registrerades integritet, kompliceras av eller riskerar att inte alls bli av på grund av att den aktuella registerlagen i alltför hög grad detaljstyr behandlingen av personuppgifter.

Att bedöma vilken normnivå som krävs för föreskrifter om behandling av personuppgifter utifrån den uttalade politiska ambitionen kan, som redan påpekats, i principiell mening vara bra för skyddet av enskildas personliga integritet. Den omständigheten att resonemang om normnivå enbart har denna utgångspunkt, och att de dessutom snarare handlar om att ha en uppfattning om författningen som sådan än om de enskilda frågor den reglerar, riskerar enligt vår mening emellertid att leda till att de integritetsfrågor som skulle behöva bli belysta från ett rättighetsperspektiv inte får den uppmärksamhet de förtjänar. Det leder i sin tur till att det blir än svårare att identifiera i vilka fall det särskilda skyddet i 2 kap. 6 § andra stycket RF verkligen ska tillämpas.

Den uttalade ambitionen att vissa registerförfattningar ska ha form av lag kan alltså paradoxalt nog leda till en sämre rättslig ana-

lys av vilka intrång i den enskildes personliga integritet som en viss behandling av personuppgifter faktiskt kan innebära.

Finns det några typfall då en behandling av personuppgifter kan anses utgöra ett intrång och därför kräva stöd i lag?

Allmänt

Den omständigheten att personuppgifter behandlas på ett sätt som omfattas av dataskyddsdirektivet kan inte i sig anses utgöra ett intrång. Det är det sammanhang där behandlingen sker som avgör om behandlingen sedd för sig kan anses utgöra ett intrång i den enskildes rätt till en privat sfär. Föreskrifter om myndigheters behandling av personuppgifter reglerar i allmänhet inte vad en myndighet ska eller tillåts göra i sin verksamhet. Detta regleras i andra regelverk som föreskriver exempelvis vilka uppgifter och vilka befogenheter myndigheten har, vilka personuppgifter och andra uppgifter som ska samlas in och från vem samt vilka uppgifter som ska lämnas till andra utanför myndighetens verksamhet. Föreskrifter om behandling av personuppgifter handlar i stället i allmänhet om vilka krav som ska ställas på sådan behandling när myndigheten utför sina uppgifter. I den mån det allmänna tillåts att göra intrång i enskildas privata sfär för att en myndighet ska kunna utföra en viss uppgift, exempelvis genom att enskilda åläggs en skyldighet att lämna uppgifter om personliga förhållanden till myndigheten, regleras detta alltså i allmänhet i något annat regelverk än i en renodlad registerförfattning. Det innebär att föreskrifter om hur behandling av personuppgifter ska gå till i allmänhet kan meddelas i form av förordning genom regeringens egen rätt att besluta föreskrifter enligt 8 kap. 7 § RF, dvs. utan att något bemyndigande om detta i lag krävs.

Det torde alltså höra till undantagen att en behandling av personuppgifter sedd för sig kan anses utgöra ett ingrepp i enskildas personliga förhållanden och därför kräver stöd i lag enligt 8 kap. 2 § första stycket 2 RF för att behandlingen ska vara tillåten.

Vad som nu sagts gäller normalt också i de fall en behandling får ske utan samtycke från den enskilde. Det finns emellertid några typsituationer där det kan finnas anledning att särskilt överväga om

det behövs stöd i lag för den avsedda behandlingen av personuppgifter.

Som redan framgått är behandling av känsliga personuppgifter utan samtycke från den enskilde ett område som enligt Europadomstolens praxis kan aktualisera frågor om intrång i den enskildes rätt till en privat sfär. Beträffande sådana uppgifter krävs därför särskilt noggranna överväganden i frågan om det behövs ett uttryckligt stöd i lag för den avsedda behandlingen. Det kan vidare konstateras att uppgiftsutbyte genom direktåtkomst, som alltså normalt medför krav på en sekretessbrytande regel som möjliggör åtkomsten, vanligtvis hämtar sitt stöd i en författning som reglerar behandling av personuppgifter. Bestämmelser som uttryckligen medger utökade befogenheter att sammanställa känsliga personuppgifter eller uppgifter om brottslighet hämtar också vanligtvis sitt stöd i en s.k. registerförfattning. Nedan behandlas mer utförligt dessa typsituationer med avseende på när det kan vara frågan om ett intrång i den enskildes personliga integritet.

Personuppgifter med ett känsligt innehåll

Behandling av känsliga personuppgifter och även uppgifter om brottslighet kan i många fall anses beröra rätten till respekt för privatlivet enligt artikel 8 i Europakonventionen. Av dataskyddsdirektivet följer att behandling av känsliga personuppgifter i princip är förbjuden, om inte den enskilde har samtyckt till behandlingen. Denna huvudregel gäller även myndigheter. I direktivet räknas upp vissa undantagsfall då en behandling utan samtycke emellertid kan vara tillåten. Vidare ger direktivet medlemsstaterna möjlighet att i sin nationella lagstiftning eller genom beslut av tillsynsmyndigheten besluta om ytterligare undantag med hänsyn till ett viktigt allmänt intresse.

I 20 § PuL har det tagits in ett bemyndigande för regeringen eller den myndighet som regeringen bestämmer att meddela undantag från förbudet att behandla känsliga personuppgifter om det behövs med hänsyn till ett viktigt allmänt intresse. Det kan konstateras att bestämmelsen utgör ett sådant bemyndigande i lag som krävs enligt 8 kap. 3 och 10 §§ RF i den mån den avsedda behand-

lingen av känsliga personuppgifter utgör ett sådant ingrepp i enskilds personliga förhållanden som avses i 2 § första stycket 2.

Genom 20 § PuL är det alltså möjligt att meddela bestämmelser som tillåter en myndighet att behandla känsliga personuppgifter med hänsyn till ett viktigt allmänt intresse i form av förordning.

Som kommer att framgå i det följande föreslår vi att det i den generella lagen ges ett generellt stöd för myndigheter att behandla känsliga personuppgifter som motiveras med att det behövs med hänsyn till ett viktigt allmänt intresse. Det kommer alltså att finnas ett uttryckligt stöd för alla myndigheter att i viss omfattning behandla känsliga personuppgifter utan samtycke från den enskilde. Bestämmelsen kompletteras med ett bemyndigande för regeringen eller den myndighet som regeringen bestämmer att meddela föreskrifter om ytterligare undantag i de fall det behövs för en viss myndighet eller en viss sektorsvis verksamhet. Det kan därför här finnas anledning att överväga i vilken utsträckning en sådan bestämmelse faktiskt innebär ett sådant intrång i enskilds personliga förhållanden som avses i 8 kap. 2 § första stycket 2 RF.

Det kan då inledningsvis konstateras att det inte kan anses givet att en behandling av känsliga personuppgifter som tillåts med hänsyn till ett viktigt allmänt intresse utgör ett intrång i den enskildes personliga integritet. I vilken mån så är fallet får bedömas utifrån det sammanhang där föreskriften ges. Om myndighetens verksamhet i övrigt är reglerad så att det redan finns bestämmelser som förutsätter eller tillåter att myndigheten använder sig av känsliga personuppgifter för att den ska kunna utföra sina uppgifter, kan det inte behövas något ytterligare stöd för det genom en bestämmelse i lag som tillåter att uppgifterna hanteras genom automatiserad behandling, dvs. elektroniskt. Exempelvis torde den behandling av känsliga personuppgifter som sker hos Försäkringskassan vara en nödvändig följd av den verksamhet som myndigheten genom andra regelverk är ålagd att utföra. Den omständigheten att uppgifterna hanteras automatiserat torde alltså inte i sig innebära ett ingrepp i enskilds personliga förhållanden. Det förhållandet att Försäkringskassans verksamhet innebär att myndigheten samlar in och bevarar känsliga personuppgifter om en stor del av befolkningen torde emellertid innebära att särskilda överväganden behöver göras beträffande ingrepp i enskilds personliga förhållanden om det exempelvis skulle bli aktuellt att ge en annan myndighet,

som inte tidigare har haft befogenhet att själv samla in den typen av uppgifter, en omfattande tillgång till Försäkringskassans informationssamlingar.

Till skillnad från det som vi betecknar som informationshanteringsförfattningar innehåller regelrätta registerförfattningar ofta en bestämmelse som föreskriver att registret i fråga ska föras. Stödet att få behandla personuppgifter i registret ges alltså i samma författning som registret har inrättats genom. Om registret innehåller känsliga personuppgifter kan därmed de föreskrifter som innebär stöd för att föra registret i sig utgöra ett ingrepp i enskilds personliga förhållanden. Ett exempel på ett sådant register med ett känsligt innehåll är belastningsregistret. Bestämmelserna i lagen (1998:620) om belastningsregister som reglerar registrets ändamål, innehåll och vilka som har rätt att få uppgifter från registret torde vara att anse som ingrepp i enskilds personliga förhållanden som kräver stöd i lag enligt 8 kap. 2 § första stycket 2 RF, medan bestämmelserna om gallring, tystnadsplikt, rätt till skadestånd m.m. syftar till att skydda den enskilde.

Andra myndigheter än den som har till uppgift att föra belastningsregistret torde sällan ha något behov av att på motsvarande sätt samla uppgifter om brottslighet. Enligt dataskyddsdirektivet är det, till skillnad från vad som gäller i fråga om känsliga personuppgifter, inte förbjudet för myndigheter att behandla personuppgifter som rör lagöverträdelser. Av de grundläggande kraven som ska vara uppfyllda vid behandling av personuppgifter torde det emellertid i allmänhet följa begränsningar i myndigheters möjligheter att i den omfattning som är syftet med belastningsregistret sammanställa den typen av uppgifter. Om någon annan myndighet än den som för belastningsregistret ska tillåtas att i en större omfattning sammanställa uppgifter om brottslighet torde det alltså behöva övervägas om det innebär ett ingrepp i enskilds personliga förhållanden som i så fall kräver stöd i lag. Av dataskyddsdirektivet följer vidare att det är förbjudet för medlemsstaterna att tillåta att ett fullständigt register över brottmålsdomar förs under kontroll av någon annan än en myndighet (artikel 8.5).

Direktåtkomst

Bestämmelser som medger direktåtkomst till känsliga personuppgifter förutsätter i allmänhet att det finns en sekretessbrytande bestämmelse som medger att uppgifterna utan någon ytterligare prövning kan lämnas ut till den som medgetts en sådan åtkomst. En sådan sekretessbrytande bestämmelse kan därför beroende på omständigheterna i det enskilda fallet utgöra ett ingrepp i den enskildes personliga förhållanden, eftersom den innebär att den sekretess som normalt ska skydda uppgifterna inte längre ska gälla i förhållande till en viss aktör som befinner sig utanför myndighetens verksamhet.

En direktåtkomst medges ofta för att effektivisera ett uppgiftsutbyte mellan myndigheter som redan äger rum. Om det tidigare uppgiftsutbytet sker med stöd av en sekretessbrytande bestämmelse som medger att uppgifter lämnas ut utan hinder av sekretess, torde den omständigheten att uppgiftsutbytet nu ska ske genom direktåtkomst inte i sig innebära att det sker något ingrepp i enskilds personliga förhållanden. Att direktåtkomst får anses vara en mer ingripande form av uppgiftsutbyte än annat elektroniskt utlämnande hänger samman med att den väcker mer allmänna frågor om verksamhetsansvar och rättsäkerhet samt – beroende på omständigheterna – i ett mer övergripande perspektiv kan sägas påverka den enskildes rätt till skydd för sina personuppgifter därför att särskilda frågor om informationssäkerhet aktualiseras (se vidare kapitel 5).

Ett uppgiftsutbyte av sekretessreglerade uppgifter som sker med stöd av den s.k. generalklausulen i 10 kap. 27 OSL, dvs. efter en avvägning mellan intresset av sekretess och den mottagande myndighetens behov av uppgifter, torde ofta inte kunna effektiviseras genom direktåtkomst utan att en ny mer definitivt sekretessbrytande bestämmelse införs som möjliggör sådan åtkomst. Eftersom en sådan sekretessbrytande bestämmelse innebär att någon intresseavvägning i det enskilda fallet inte längre ska göras, kan det uppfattas innebära en försvagning av sekretesskyddet vilket i sin tur kan utgöra ett ingrepp i enskilds personliga förhållanden. Ett uppgiftsutbyte mellan myndigheter med stöd av 10 kap. 27 § OSL kan emellertid ofta vara av sådant slag att det redan finns författningsstöd för det genom en bestämmelse i lag eller förordning som medger att uppgifter rutinmässigt får lämnas ut. Utbytet kan också ha

sådan karaktär att uppgifter efter en intresseavvägning i praktiken alltid kan lämnas ut. Den omständigheten att en ny sekretessbrytande bestämmelse behöver införas för att möjliggöra att utbytet effektiviseras genom direktåtkomst behöver i ett sådant fall inte heller innebära ett ingrepp i enskildas personliga förhållanden.

Den omständigheten att direktåtkomst medges torde alltså många gånger inte i sig innebära att det sker något ingrepp i enskilds personliga förhållanden i den mening som avses i 8 kap. 2 § första stycket 2 RF. Föreskrifter om att direktåtkomst får medges torde därför som huvudregel kunna ges i förordning. Om direktåtkomsten emellertid förutsätter att enskildas sekretesskydd i realiteten försvagas på så sätt att känsliga personuppgifter kan lämnas ut i betydligt större omfattning än vad som annars hade varit möjligt kan den emellertid vara att anse som ett sådant ingrepp i enskildas personliga förhållanden som förutsätter stöd i lag.

Av betydelse för om en direktåtkomst kan anses utgöra ett ingrepp i enskilds personliga förhållanden eller inte är naturligtvis också vilket förhållande de myndigheter har till varandra mellan vilket uppgiftsutbytet sker. Om myndigheternas verksamheter har nära anknytning till varandra och förutsätter att ett visst uppgiftsutbyte sker för att respektive myndighet ska kunna utföra sina uppgifter talar detta för att en direktåtkomst mellan dessa myndigheter inte i sig utgör ett ingrepp i enskilds personliga förhållanden. Som exempel kan nämnas det uppgiftsutbyte som sker mellan Skatteverkets beskattningsverksamhet, Kronofogdemyndigheten och Tullverket, med bortseende från deras brottsutredande verksamhet. Om däremot brottsbekämpande myndigheter medges direktåtkomst till sekretessreglerade personuppgifter hos myndigheter som inte ägnar sig åt brottsbekämpning torde det regelmässigt vara frågan om ett ingrepp i enskilds personliga förhållanden som kräver stöd i lag, såvida inte uppgiftsutbytet är av ringa omfattning.

Sammanställningar av känsliga personuppgifter

I många registerförfattningar finns bestämmelser som begränsar myndigheters möjligheter att söka efter och sammanställa känsliga personuppgifter, s.k. sökbegränsningar. Redan av dataskyddsdirektivets regler om vilka grundläggande krav som ska uppfyllas vid en

behandling av personuppgifter följer visserligen begränsningar i möjligheterna att sammanställa personuppgifter på så sätt att sammanställningen ska vara förenlig med det ändamål för vilket uppgifterna samlades in. Uppgifterna ska också vara relevanta i förhållande till ändamålet med sammanställningen och inte fler än vad som är nödvändigt för ändamålet. I en myndighets verksamhet åligger det alltså den som behandlar personuppgifter att göra dessa överväganden innan en sammanställning görs. Genom en bestämmelse som föreskriver vissa sökförbud har emellertid lagstiftaren som vi ser det gjort denna bedömning ”på förhand” och klargjort att vissa sammanställningar inte ska få ske hos myndigheten. Sådana sökförbud innebär också begränsningar i enskildas möjlighet att få en sammanställning gjord med stöd av reglerna om allmänna handlingar i 2 kap. TF (jfr 2 kap. 3 § tredje stycket). Om en myndighet däremot bedöms ha behov av att kunna göra sådana sammanställningar för att utföra sina uppgifter och att det därför behöver införas en uttrycklig bestämmelse som tillåter det, kan detta beroende på omständigheterna måhända anses utgöra ett ingrepp i enskilds personliga förhållanden. Det ändamål för vilket sammanställningen tillåts ske torde vara avgörande för om det ska vara att anse som ett ingrepp i enskilds personliga förhållanden eller inte.

När kan behandling av personuppgifter vara ett betydande intrång?

Ovan har vi behandlat frågan om när behandling av personuppgifter i sig kan anses utgöra ett sådant ingrepp i enskilds personliga förhållanden att det enligt 8 kap. 2 § första stycket 2 RF kräver stöd i lag. Nästa fråga blir då i vilken mån sådan behandling också eller därutöver kan anses utgöra ett betydande intrång i den mening som avses i 2 kap. 6 § andra stycket RF och i övrigt uppfyller de förutsättningar som anges i stadgandet, dvs. sker utan samtycke och innebär kartläggning eller övervakning av den enskildes personliga förhållanden. Om grundlagsstadgandet är tillämpligt innebär det att kravet på lagform är obligatoriskt – dvs. bemyndiganden är uteslutna – och att de särskilda begränsningarna enligt 2 kap. 20–22 §§ RF rörande förutsättningarna för riksdagen att besluta lagen gäller.

I 2 kap. 6 § första stycket RF räknas upp ett antal fall av intrång i den enskildes personliga integritet som ansetts kräva särskilt begränsande regler för att de ska kunna tillåtas genom lag. Det handlar exempelvis om kroppsvisitation, husrannsakan och hemlig avlyssning. I dessa fall är det alltså frågan om metoder för insamling av uppgifter om personliga eller ekonomiska förhållanden som ansetts utgöra särskilt svåra intrång i vars och ens rätt till en privat sfär. Vi har ovan konstaterat att behandling av personuppgifter däremot inte utgör en metod eller teknik som i sig innebär intrång i enskildas personliga integritet, utan att det är det sammanhang där behandlingen sker som avgör om så är fallet.

Inledningsvis kan påpekas att 2 kap. 6 § andra stycket RF till sin ordalydelse inte särskilt tar sikte på behandling av personuppgifter. Tillämpningsområdet avser, liksom 8 kap. 2 § första stycket 2 RF, ”personliga förhållanden”. Ordalydelsen saknar referenser till inrättandet och förandet av personregister även om det av motiven framgår att det är ett slag av verksamhet som har avsetts träffas av bestämmelsen. I motiven framhålls att vad som ska avses med ”kartläggning” och ”övervakning” får bedömas med vad som enligt normalt språkbruk läggs i dessa begrepp. Det leder knappast tanken till personuppgiftsbehandling som sådan. Samtidigt finns det, som har framgått, motivuttalanden som kan sägas ge uttryck för att redan det förhållandet att omfattande eller känsliga informationsmängder hanteras hos en viss myndighet kan ses som ett slags kartläggning som är av det slaget att grundlagsbestämmelsen ska anses vara tillämplig.

Det går alltså knappast att utifrån grundlagsstadgandets ordalydelse avgöra i vilken mån stadgandet är tillämpligt på personuppgiftsbehandling sedd för sig. Vad som kan komma att anses gälla här lär få utmejslas i det framtida lagstiftningsarbetet. Ytterst avgörs saken av konstitutionsutskottet som för riksdagens del prövar om ett visst lagförslag utgör en fri- och rättighetsbegränsning eller inte (jfr 2 kap. 22 § tredje stycket RF).

Av ställningstaganden som hittills gjorts i vissa lagstiftningsärenden rörande tillämpningen av stadgandet kan emellertid den slutsatsen dras att när en ny uppgift åläggs en myndighet uppgiften, beroende på omständigheterna, kan uppfattas som en sådan integritetskränkande behandling som omfattas av grundlagsbestämmelsen. En viss skyldighet för en brottsbekämpande myndighet att

lämna uppgifter till en annan sådan myndighet har t.ex. ansetts inte vara omfattat av grundlagsstadgandet så länge de båda myndigheterna är svenska. Förhållandet har emellertid ansetts vara det motsatta om uppgifterna ska lämnas till en brottsbekämpande myndighet i utlandet. I båda fallen är fråga om en behandling av personuppgifter men det är alltså inte denna omständighet utan snarare den sakliga innebörden av åtgärden – att uppgifter ska utbytas – som har ansetts utslagsgivande för om det ska vara frågan om ett betydande intrång.

Enligt vår mening förefaller det naturligt att vid bedömningen av om grundlagsstadgandet är tillämpligt eller inte på det sättet utgå från den sakliga innebörden av en viss tänkt reglering. Lagstiftaren får således ställa sig frågan vad det är som avses ska ske. Om bedömningen då blir att en viss myndighetsuppgift träffas av grundlagsstadgandet innebär detta att den uppgiften behöver regleras i lag och att de särskilda förutsättningarna för rättighetsbegränsade lagstiftning i 2 kap. RF då gäller. Det innebär däremot inte att all personuppgiftsbehandling som sker vid myndigheten i fråga nödvändigtvis kräver lagstöd. Det är alltså, som vi ser det, fråga om samma slags bedömning som behöver göras för att avgöra om en behandling av personuppgifter i sig utgör ett sådant ingrepp i enskilds personliga förhållanden som avses i 8 kap. 2 § första stycket 2 RF, dock att det nu också ska bedömas om det är frågan om ett betydande intrång.

Som framgått har det emellertid förekommit att lagstiftaren intagit den positionen att den behandling av personuppgifter som sker vid en viss myndighet till ”stora delar” är av det slaget att grundlagstadgandet blir tillämpligt och att därför all den personuppgiftsbehandling som sker vid myndigheten har reglerats i lag, dvs. utöver det författningsstöd som redan finns för den faktiska verksamhet som myndigheten bedriver.

Det ska dock framhållas att grundlagstadgandet knappast kräver att lagstiftaren på detta sätt gör en avvägning av om en hel reglering för en viss verksamhet ska ha form av lag eller förordning. Det är som vi ser det endast de moment i verksamheten som utgör ett betydande intrång och i övrigt uppfyller förutsättningarna enligt stadgandet som måste ha stöd i lag. Det lagstiftningsärende där datalagringsdirektivet infördes i svensk rätt innebar inte någon ny skyldighet för en myndighet när det gäller behandling av uppgifter

som rör enskilds personliga förhållanden, utan skyldigheten tog sikte på leverantörer av elektroniska kommunikationstjänster, dvs. enskilda aktörer. Emellertid syftade skyldigheten att lagra s.k. trafikuppgifter till att brottsbekämpande myndigheter skulle ha tillgång till uppgifterna för sin verksamhet. På så sätt rörde skyldigheten förhållandet mellan enskilda och det allmänna. Redan den lagring av vars och ens trafikuppgifter som leverantörerna blev ålagda att utföra ansågs utgöra ett intrång i enskildas personliga integritet. Mot bakgrund av den mängd trafikuppgifter om en enskild som kunde komma att lagras, ansågs intrånget också vara betydande.

Datalagringen torde utgöra ett tydligt exempel på ett fall då grundlagsstadgandet blir tillämpligt med hänsyn till både det sätt som valdes för att brottsbekämpande myndigheter skulle ha möjlighet att få tillgång till trafikuppgifter, nämligen att enskilda aktörer ålades att för brottsbekämpande ändamål lagra de uppgifter som de ursprungligen samlat in för att kunna utföra tjänster i förhållande till sina kunder, samt omfattningen av lagringen och uppgifternas integritetskänsliga karaktär.

Vi har för vår del svårt att se att grundlagsstadgandet kan ges den innebörden att det – bortsett från de brottsbekämpande myndigheterna – kan finnas myndigheter eller kategorier av myndigheter vilkas verksamhet är av det slaget att all den behandling av personuppgifter som äger rum där måste ha stöd i en sådan lag som endast får beslutas enligt reglerna i 2 kap. RF. Det förefaller också vara i rena undantagsfall som behandling av personuppgifter hos icke brottsbekämpande myndigheter kan anses innehålla några särskilda moment av personuppgiftsbehandling som typiskt sett kan ses som en sådan kartläggning eller övervakning som innebär ett betydande intrång i den personliga integriteten och därför omfattas av grundlagsstadgandet.

Sammanfattning

Från allmän normgivningssynpunkt ser vi inga hinder mot att bestämmelser som avviker från eller kompletterar innehållet i den generella lagen i form av t.ex. myndighetsspecifika föreskrifter om sökbegränsningar, direktåtkomst, behandling av känsliga personuppgifter m.m. ges i förordningsform. I den mån sådana bestämmelser

innebär åligganden för de kommunala myndigheterna krävs emellertid att bemyndiganden tas in i lagen (jfr 8 kap. 2 § första stycket 3 RF). Detsamma gäller förstås också beträffande sådana regleringar som är att se som ingrepp i enskilds personliga förhållanden. Vi återkommer till frågan om hur erforderliga bemyndiganden bör utformas i avsnitt 18.2.

Det torde bara vara i rena undantagsfall som något visst moment av behandling av personuppgifter i sig är att se som ett sådant betydande intrång att grundlagsstadgandet om skydd för den personliga integriteten blir tillämpligt och regleringen därför måste ges i lag och beslutas i enlighet med 2 kap. RF. I den mån det finns sådana moment i myndighets- eller sektorsspecifik behandling av personuppgifter som anses utgöra ett sådant betydande intrång kan bestämmelser om detta ges lagform genom att tas in i bilaga till den generella lagen. Om det skulle anses mer ändamålsenligt att behandlingen regleras i en egen författning, t.ex. för att det är frågan om hur ett visst integritetskänsligt register ska få föras snarare än att reglera hur personuppgifter får behandlas i en viss myndighetsverksamhet, kan regleringen givetvis också ges i en särskild lag som därmed gäller före den generella lagens bestämmelser.

Oavsett hur en viss reglering ska bedömas i normgivningshänseende är det naturligtvis inget som hindrar att myndighetsspecifika föreskrifter av lämplighetsskäl eller andra skäl ändå bedöms bör ges i lag. Sådana föreskrifter – liksom föreskrifter som faktiskt kräver lagstöd och där den bedömningen görs att det av något skäl inte är lämpligt att utnyttja ett bemyndigande – kan också tas in i bilaga till den generella lagen.

8 Allmänna bestämmelser

8.1 En bestämmelse om lagens syfte

8.1.1 Bakgrund

Både i dataskyddsdirektivet och i personuppgiftslagen finns inledande bestämmelser om vilket övergripande syfte respektive reglering har. Sådana syftesbestämmelser förekommer även i en del registerförfattningar.

Dataskyddsdirektivet

I artikel 1 i direktivet föreskrivs under rubriken Direktivets syfte att medlemsstaterna ska i enlighet med direktivet skydda fysiska personers grundläggande fri- och rättigheter, särskilt rätten till privatliv, i samband med behandling av personuppgifter. Vidare får medlemsstaterna varken begränsa eller förbjuda det fria flödet av personuppgifter mellan medlemsstaterna av skäl som har samband med det nyss nämnda föreskrivna skyddet. Det bakomliggande syftet med dataskyddsdirektivet brukar anges vara att åstadkomma ett fritt flöde av personuppgifter inom Europeiska unionen. Det syftet ska uppnås genom en harmonisering av medlemsstaternas lagstiftning för att få en likvärdig skyddsnivå för enskilda personers fri- och rättigheter, särskilt rätten till privatliv, med avseende på behandling av personuppgifter.

Personuppgiftslagen

I 1 § anges att personuppgiftslagens syfte är att skydda människor mot att deras personliga integritets kränks genom behandling av personuppgifter. Eftersom ett fritt flöde av personuppgifter mellan

medlemsstaterna i Europeiska unionen åstadkoms genom en åtminstone delvis harmoniserad lagstiftning till skydd mot kränkning av personlig integritet genom behandling av personuppgifter, ansågs det vid personuppgiftslagens införande inte motiverat att särskilt upplysa även om det fria flödet som ett särskilt syfte (prop. 1997/98:44 s. 115).

Förslaget till uppgiftsskyddsförordning

Det pågående reformarbetet syftar inte till något avsteg från vad som slogs fast om det grundläggande syftet med dataskyddsdirektivet. Förordningens artikel 1 – med rubriken Syfte och mål – har visserligen modifierats något i struktur och ordalydelse i jämförelse med artikel 1 i direktivet. Någon ändring i sak torde detta inte innebära.

I förordningsförslaget (bl.a. motiveringen s. 1 och punkterna 5 och 6 i ingressen) framhålls att den snabba utvecklingen av informationstekniken har omvandlat såväl ekonomin som samhällslivet inom EU. Vidare framhålls att förändringarna kräver en stark och mer sammanhängande ram för uppgiftsskyddet, uppbackad av ett kraftfullt tillsynsarbete, eftersom det är viktigt att skapa den tillit som behövs för att utveckla den digitala ekonomin över hela den inre marknaden. Enskilda bör ha kontroll över sina egna personuppgifter och rättssäkerheten och smidigheten för enskilda, ekonomiska operatörer och myndigheter bör stärkas. Enligt kommissionen är det avgörande för den ekonomiska utvecklingen att bygga upp förtroendet för nätmiljön. Bristande förtroende gör att konsumenter tvekar att ”köpa på nätet” och att använda nya tjänster. Detta kan hämma utvecklingen av innovativa användningar av ny teknik. Skydd av personuppgifter spelar därför en central roll i den digitala agendan för Europa och mer allmänt i Europa 2020-strategin (se avsnitt 3.1.4).

Det kan således konstateras att informationstekniken ges en framskjuten betydelse för en önskvärd samhällsutveckling på bred front. En robust dataskyddsreglering är inte bara ett mål i sig utan också ett medel att uppnå en önskad samhällsutveckling i ett längre perspektiv.

Registerförfattningar

I registerförfattningar förekommer ibland bestämmelser som anger lagens övergripande syfte.

När det gäller informationshanteringsförfattningar förekommer syftesbestämmelser framför allt i sådana författningar som ersätter personuppgiftslagen och sedan hänvisar till olika bestämmelser i personuppgiftslagen som ska ha motsvarande tillämpning då personuppgifter behandlas inom ramen för informationshanteringsförfattningens tillämpningsområde.

I exempelvis 1 kap. 1 § polisdatalagen (2010:361) anges det övergripande syftet med lagen vara att ge polisen möjlighet att behandla personuppgifter på ett ändamålsenligt sätt i sin brottsbekämpande verksamhet och att skydda människor mot att deras personliga integritet kränks vid sådan behandling. Enligt motiven (prop. 2009/10:85 s. 66 f.) avspeglar utformningen av bestämmelserna den avvägning mellan å ena sidan intresset av en effektiv brottsbekämpning och å andra sidan intresset av skydd för den personliga integriteten som gjorts i lagstiftningsärendet. I 1 kap. 1 § kustbevakningsdatalagen (2012:145) finns en motsvarande bestämmelse om lagens syfte. Det finns dock exempel på informationshanteringsförfattningar med samma lagtekniska konstruktion vad avser förhållandet till personuppgiftslagen som varken hänvisar till 1 § PuL eller har en egen syftesbestämmelse.

I sådana informationshanteringsförfattningar som är konstruerade på det sättet att personuppgiftslagen gäller i den mån författningen i fråga inte innehåller avvikande bestämmelser förekommer i allmänhet inte någon särskild syftesbestämmelse som ersätter eller gäller utöver vad som sägs i 1 § PuL.

Beträffande renodlade registerförfattningar förekommer bestämmelser som anger författningens syfte eller ett visst registers syfte. För de så kallade publicitetsregistren anges ofta att registret ska ”ge offentlighet åt” ett visst förhållande, se t.ex. 1 § lagen (2000:224) om fastighetsregister eller 2 kap. 1 § aktiebolagsförordningen (2005:559).

8.1.2 Våra överväganden och förslag

Förslag: I den nya lagen införs en bestämmelse som anger vilket syfte lagen har. Detta är tudelat. Syftet är att dels ge myndigheter möjlighet att behandla personuppgifter på ett ändamålsenligt sätt i deras verksamheter, dels skydda människor mot att deras personliga integritet kränks vid sådan behandling.

Bestämmelser om lagars syfte saknar normalt egentligt materiellt innehåll utan framstår mer som ett slags deklaration av de bakomliggande och övergripande målen med de efterföljande lagbestämmelserna med mer konkret reglering. Man kan därför fråga sig om det verkligen behövs en syftesbestämmelse av detta slag i den nya lagen. Onekligen har emellertid en syftesbestämmelse en informativ och pedagogisk betydelse.

Ett uttryckligt fastslående av lagens syfte har emellertid inte enbart en symbolisk eller informativ betydelse. Att en lags syfte anges i lagen kan få relevans i rättstillämpningen genom att ge vägledning för tolkningen av de materiella bestämmelserna i lagen. Vidare klargör en sådan bestämmelse att lagen enbart innehåller sådana bestämmelser som är av dataskyddsrättslig karaktär.

Sammanfattningsvis anser vi således att det finns skäl att ta in en bestämmelse om lagens syfte i den nya lagen.

Hur bör lagens syfte anges?

En syftesbestämmelse måste av naturliga skäl vara övergripande. Vi bedömer att en bestämmelse som föreskriver att lagens syfte är att dels ge myndigheterna möjlighet att behandla personuppgifter på ett ändamålsenligt sätt, dels skydda människor mot att deras personliga integritet kränks vid myndigheternas informationshantering väl fångar regleringens målsättning på ett sätt som passar för alla myndigheter oavsett vad för slags verksamhet de bedriver.

Syftet att ge möjligheter till en ändamålsenlig personuppgiftsbehandling är viktigt att framhålla. För myndigheter är det av helt avgörande betydelse att kunna behandla personuppgifter genom elektronisk informationshantering för att utföra sina uppgifter i överensstämmelse med de krav som ställs på bl.a. rättssäkerhet,

effektivitet och en önskvärd servicenivå. Detta kan inte sällan innebära att myndigheter exempelvis måste ges större förutsättningar att behandla personuppgifter utan den registrerades samtycke än vad som gäller utanför den offentliga sektorn. Den nya lagen med anknytande föreskrifter kommer att innehålla bestämmelser som skapar sådana förutsättningar.

Vad som är en ändamålsenlig personuppgiftsbehandling kan inte slås fast i generella termer utan varierar i hög grad beroende på vad för slags verksamhet det handlar om.

Det andra ledet i den föreslagna syftesbestämmelsen – att lagens syfte är att skydda människor mot att deras personliga integritet kränks vid myndigheters personuppgiftsbehandling – är av central betydelse. Genom syftesbestämmelsen kommer detta till uttryck i lagen. Härigenom framgår vidare indirekt att verksamhetsreglering av olika slag faller utanför lagens syfte. Lagens bestämmelser ska enbart inriktas på att reglera informationshanteringen i förhållande till det skydd som personuppgiftsbehandling påkallar.

Att myndigheters behandling av personuppgifter inte medför kränkningar av människors personliga integritet är alltså en central målsättning för regleringen. Samtidigt är vissa intrång nödvändiga för att myndigheterna ska kunna utföra sina uppgifter. Regleringen bör därför ge uttryck för en väl avvägd balans och proportionalitet mellan, å ena sidan, samhällets behov av att myndigheter kan behandla personuppgifter i sin verksamhet och, å andra sidan, skyddet för den personliga integriteten. Ett gott integritetsskydd är av fundamental betydelse för att myndigheterna alls ska kunna ges förutsättningar att behandla personuppgifter med ett bevarat förtroende från allmänhetens sida. På ett övergripande plan kan det alltså sägas finnas ett samspel mellan integritetsskydd och förutsättningar för en ändamålsenlig informationshantering. Detta tydliggörs genom den tudelade syftesbestämningen – ändamålsenlighet respektive integritetsskydd – och illustrerar att de båda målen gäller parallellt.

8.2 Lagens tillämpningsområde

8.2.1 Vilka myndigheter bör omfattas av lagens tillämpningsområde?

Förslag: Lagen ska i princip tillämpas av alla myndigheter. Med myndigheter avses i lagen detsamma som i regeringsformen, dvs. alla statliga och kommunala organ utom riksdagen och de beslutande kommunala församlingarna.

Vi har i avsnitt 7.2 redogjort för varför det bör införas en samlad lag för myndigheterna med generella bestämmelser till skydd för personuppgifter.

Enligt vår mening talar övervägande skäl för att lagen bör vara tillämplig hos alla slags myndigheter och inte t.ex. bara sådana som i dag omfattas av särskilda registerförfattningar. Det är enligt vår mening angeläget att ett och samma grundläggande regelverk gäller inom hela myndighetssektorn. Att samma grundläggande regler för behandling av personuppgifter gäller för alla myndigheter ger ökad tydlighet och transparens. Det ger också bäst förutsättningar för effektivitetshöjande myndighetsgemensamma lösningar, exempelvis uppgiftsbyte myndigheter emellan.

Att alla myndigheter kommer att omfattas av lagens tillämpningsområde är också ägnat att väsentligt underlätta den reformering av regelverket som kommer att behöva göras som ett resultat av det pågående reformarbetet inom EU som kan förväntas leda till att dataskyddsdirektivet ersätts av en allmän uppgiftsskyddsförordning.

Med myndigheter avses här detsamma som i regeringsformen, dvs. alla statliga och kommunala organ utom riksdagen och de beslutande kommunala församlingarna.

8.2.2 Vilka verksamheter bör omfattas av lagens tillämpningsområde?

Förslag: Vissa verksamheter undantas från lagens tillämpningsområde nämligen

- en myndighets administrativa verksamhet,
- en myndighets verksamhet som personuppgiftsbiträde, och
- sådan verksamhet som bedrivs av behöriga myndigheter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller beivra brott eller verkställa straffrättsliga påföljder.

Våra direktiv är öppna i fråga om tillämpningsområdet. I direktiven klargörs emellertid att den brottsbekämpande verksamheten inte omfattas av utredningsuppdraget. Ett skäl till detta är att den verksamheten inte omfattas av förslaget till allmän uppgiftsskyddsförordning utan av ett förslag till direktiv om uppgiftsskydd i den brottsbekämpande verksamheten. Härmed avses verksamhet som bedrivs av behöriga myndigheter i syfte att förebygga, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder (se artikel 2.2 e i uppgiftsskyddsförordningen, jfr även artikel 1.2 i gällande dataskyddsrambeslut). För Polismyndigheten, Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten, Kriminalvården och Övervakningsnämnderna är brottsbekämpande verksamhet den dominerande uppgiften. Även Kustbevakningen, Skatteverket och Tullverket har uppdrag att bedriva brottsbekämpande verksamhet. De allmänna domstolarnas verksamhet på det straffrättsliga och straffprocessuella området hör också till den brottsbekämpande verksamheten i här aktuell bemärkelse.

Den brottsbekämpande verksamheten ska alltså inte omfattas av lagens tillämpningsområde. Till bilden hör vidare att den brottsbekämpande verksamheten till stora delar nyligen genomgått eller genomgår en översyn av regleringen av personuppgiftsbehandling. Polisdatalagen och kustbevakningsdatalagen är tämligen nya författningar och det pågår lagstiftningsarbete bl.a. såvitt avser Åklagarmyndigheten samt beträffande Tullverkets brottsbekämpande verksamhet. Registerförfattningsregleringen av den brottsbekämpande

verksamheten är emellertid inte i alla delar heltäckande. Exempelvis förekommer behandling av personuppgifter med stöd av personuppgiftslagen i brottsbekämpande verksamhet vid Nationellt forensiskt centrum, en enhet inom Polismyndigheten.

Nästa fråga blir då om personuppgiftsbehandling i all slags övrig myndighetsverksamhet än den som uttryckligen undantagits från utredningsuppdraget bör omfattas av den nya lagens tillämpningsområde.

Det säger sig självt att myndigheters behandling av personuppgifter sker i varierande och mångfacetterade verksamheter. Redan de registerförfattningar som finns i dag spänner över en mycket brokig verksamhetskarta som innefattar myndighetsverksamhet inom såväl staten som landstingen och kommunerna. Både myndigheters handläggning av ärenden samt s.k. faktiskt handlande (t.ex. vård av en patient eller en myndighets serviceverksamhet enligt 4 § FL) omfattas inte sällan av informationshanteringsförfattningar. Båda slagen av verksamhet, som inte alltid är så lätta att avgränsa, bör enligt vår mening omfattas av den nya lagens tillämpningsområde. Behandling av personuppgifter behövs emellertid inte bara i den egentliga sakverksamheten utan även för t.ex. övergripande planering, verksamhetsuppföljning och egentillsyn. Normalt handlar det då om ”återanvändning” genom olika slags bearbetning av personuppgifter som redan samlats in i den löpande verksamheten. Även sådan behandling bör omfattas av lagen, eftersom det ingår i myndigheternas ansvar att planera, administrera och kvalitetssäkra sin verksamhet. Det är vår uppfattning att utgångspunkten bör vara att den nya lagen ska gälla, om det inte föreskrivits något undantag eller annat följer av avvikande bestämmelser. I linje härmed anser vi att det inte bör införas någon beskrivning av vilka verksamhetsområden som omfattas av lagens tillämpningsområde. Verksamhetsområdet ska i stället framgå motsatsvis.

I fråga om vilka undantag som uttryckligen bör föreskrivas, utöver den brottsbekämpande verksamheten, gör vi följande överväganden.

Generellt gäller på registerlagstiftningsområdet att den personuppgiftsbehandling som sker i myndigheternas rent administrativa verksamhet med t.ex. personal- och lokalfrågor, materialförsörjning och ekonomiadministrativa göromål utan närmare koppling till sakverksamheten faller utanför den särreglering som register-

författningarna omfattar. Detta brukar framgå indirekt av det sätt som registerförfattningens tillämpningsområde beskrivs på samt av förarbetsuttalanden (se t.ex. 1 § studiestödsdatalagen och prop. 2008/09:96 s. 76). Vi menar att det är naturligt att den rent internadministrativa verksamheten med t.ex. personal-, lokal- och ekonomiadministration även framgent regleras av personuppgiftslagen i stället för av den nya lagen. I myndigheternas administration behandlas nämligen inte personuppgifter som samlats in då myndigheterna fullgör de uppgifter som de är ålagda att utföra inom ramen för deras verksamhet. Myndigheternas administration är därmed i princip likställd den som sker hos enskilda personuppgiftsansvariga i rollen som t.ex. arbetsgivare och påkallar inte en särreglering i förhållande till den allmängiltiga regleringen i personuppgiftslagen. Visserligen finns det skillnader, hos myndigheter genereras exempelvis allmänna handlingar även inom personaladministrationen, men de skillnader som finns utgör enligt vår mening knappast tillräckliga skäl för att avvika från den ordning som hittills gällt. Det sagda innebär att myndigheternas administrativa verksamhet bör undantas från den nya lagens tillämpningsområde.

Av stor vikt för den samlade regleringens konsekvens och begriplighet är att bestämmelserna har en tydlig adressat. Det förekommer registerförfattningar som är otydliga på den punkten. Ett exempel är studiestödsdatalagen som enligt lagens bestämmelse om tillämpningsområde bara gäller för Centrala studiestödsnämndens verksamhet (1 § studiestödslagen). Dock är lagens bestämmelse om direktåtkomst så avfattad att den tycks rikta sig till mottagande myndigheter genom att reglera hur deras direktåtkomst till nämndens personuppgiftssamlingar får användas. Den samlade reglering som vi föreslår bör vara tydlig på denna punkt. Lagen ska i allt väsentligt därför enbart ta sikte på de förutsättningar och skyldigheter som gäller för en personuppgiftsansvarig myndighet. Bestämmelsernas adressat ska alltså genomgående vara den myndighet som är personuppgiftsansvarig.

Som närmare kommer att behandlas i avsnitt 10.1 förekommer emellertid att myndigheter behandlar personuppgifter såsom personuppgiftsbiträde till en personuppgiftsansvarig, vilken kan vara såväl en annan myndighet som en enskild. För att uppnå den eftersträvade tydligheten angående vem som är skyldig att följa lagens bestämmelser, eller se till att lagens bestämmelser följs, bör per-

sonuppgiftsbehandling som en myndighet utför i egenskap av personuppgiftsbiträde därför undantas från lagens tillämpningsområde. Det är sedan en annan sak att lagens bestämmelser i praktiken ändå kommer att gälla även för en myndighet som är personuppgiftsbiträde om den personuppgiftsansvarige är en myndighet vars behandling omfattas av lagen. Förhållandet blir dock ett annat då den personuppgiftsansvarige är en enskild aktör.

Det förekommer ibland att en myndighet utan att vara personuppgiftsbiträde behandlar personuppgifter genom sådan teknisk lagring eller teknisk bearbetning för annan myndighets räkning som avses i 2 kap. 10 § första stycket TF. Det kan vara fråga om såväl en begränsad it-tjänst som överlämnande av hela it-driften. Vi ser dock inte anledning att föreslå något undantag för en myndighets verksamhet med att lagra eller bearbeta upptagningar med personuppgifter för annans räkning som motsvarar undantaget för myndigheters personuppgiftsbehandling såsom personuppgiftsbiträde. Den nya lagens tillämpningsområde kommer således att omfatta en myndighets behandling bestående av lagring eller bearbetning för annans räkning som avses i 2 kap. 10 § första stycket TF.

I våra direktiv berörs inte frågan om vad som bör gälla beträffande personuppgiftsbehandlingar inom de delar av den offentliga sektorn som inte omfattas av den unionsrättsliga regleringen, t.ex. inom försvarsområdet. Från det materiella tillämpningsområdet för uppgiftsskyddsförordningen undantas, utöver brottsbekämpande verksamhet, enligt artikel 2 bl.a. behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av unionslagstiftningen, särskilt avseende nationell säkerhet, eller som medlemsstaterna utför när de bedriver verksamhet som omfattas av kapitel 2 i EU-fördraget (som innehåller särskilda bestämmelser om den gemensamma utrikes- och säkerhetspolitiken).

Dataskyddsdirektivets materiella tillämpningsområde är på motsvarande sätt begränsat (artikel 3).

Personuppgiftslagen är däremot tillämplig även på verksamheter som inte omfattas av unionsrätten. I förarbetena anfördes bl.a. att en begränsning av lagens tillämpningsområde till vad som krävs enligt direktivet skulle strida mot vad som tillämpats under lång tid i Sverige, nämligen ett system som utgår från en generell lag kompletterad med särregler i s.k. registerförfattningar. Om viss offentlig verksamhet skulle generellt undantas från personuppgiftslagen, fanns det risk

för att viss behandling inom den offentliga sektorn inte skulle komma att omfattas av någon lagstiftning med motsvarande syfte som den lagen. Personuppgiftslagen gjordes därför generellt tillämplig till att omfatta även verksamhet utanför det som numera benämns unionsrätten (prop. 1997/98:44 s. 40).

Vårt uppdrag innebär, som tidigare framgått, att utforma en reglering som är väl anpassad till den pågående dataskyddsreformen inom EU. Om möjligt ska vi skapa en reglering som kan fungera som ett komplement till den unionsrättsliga regleringen på området. Detta skulle kunna tala för att en kommande anpassning av den föreslagna lagen till uppgiftsskyddsförordningen underlättas om lagens tillämpningsområde överensstämmer med uppgiftsskyddsförordningens. Därmed skulle det inte finnas någon risk för att ett inordnande i den föreslagna lagen av verksamhet som faller utanför unionsrätten bara blir en temporär ordning. Genomförandet av uppgiftsskyddsförordningen förefaller emellertid inte vara nära förestående och under alla förhållanden kan det antas, mot bakgrund av vad som nu är känt om innehållet i den kommande förordningen, att det kommer att finnas ett tämligen stort utrymme för nationell reglering av myndigheters behandling av personuppgifter. Det finns därmed, menar vi, goda förutsättningar för att finna en lösning för hur lagen bör anpassas till den kommande uppgiftsskyddsförordningen utan hinder av att även verksamhet som inte omfattas av unionslagstiftningen ingår i lagens tillämpningsområde. Vi anser därför att det stora värde ur tillämpningssynpunkt som finns i en så långt möjligt samlad reglering för enskilda myndigheters behandling av personuppgifter – alldeles oavsett om verksamheten omfattas av unionsrätten eller inte – väger tyngre än de komplikationer som måhända kan uppstå i samband med ett införande av uppgiftsskyddsförordningen. Vi bedömer därför att tillämpningsområdet inte bör begränsas till myndighetsverksamhet som omfattas av unionsrätten. I avsnitt 19.2.3 återkommer vi till frågan om lagens tillämpningsområde.

8.2.3 Lagens förhållande till befintliga registerförfattningar m.m.

Förslag och bedömning: Lagen ska – med undantag för personuppgiftslagen och bestämmelser som meddelats med stöd av den lagen – vara subsidiär i förhållande till bestämmelser i annan lag eller förordning som avviker från lagens bestämmelser. Befintliga registerförfattningar fortsätter därför att vara tillämpliga även efter lagens införande. Lagens tillämpningsområde vid ikraftträdandet blir därmed sådan personuppgiftsbehandling hos myndigheter som sker med stöd av personuppgiftslagen. Avsikten är emellertid att dataskyddsrättslig särreglering i form av registerförfattningar efter hand bör upphävas eller i vart fall förenklas och att den nya lagen därmed blir tillämplig i stället. Eventuella behov av fortsatt särreglering kan tillgodoses genom att sådana bestämmelser tas in i en till lagen anslutande förordning eller vid behov, i bilaga till lagen.

Flertalet regelrätta registerförfattningar innehåller verksamhetsreglering i det avseendet att de tilldelar en myndighet uppgiften att vara registerhållare och därutöver innehåller närmare regler om uppgifter som ska hämtas in, registreras osv., dvs. regler som inte tar sikte på personuppgiftsbehandling som sådan. Som har framgått av avsnitt 7.2 menar vi att den nya lagen enbart bör innehålla bestämmelser som utgör dataskyddsregler och att nyss nämnda registerförfattningar inte bör beröras förutom i de delar som avser dataskyddsreglering. Det finns ett flertal sådana reglerade register inom olika sektorer, t.ex. receptregistret, fastighetsregistret, handelsbolagsregistret, olika hälsodataregister m.m. Nya sådana register kommer att behöva inrättas och därmed regleras. Vi ser, som redan sagts, ingen anledning att ha som ambition att försöka ersätta den typen av regelrätta registerförfattningar genom att i stället reglera verksamhetsspecifika registerfrågor i anslutning till den nya lagen. Som har framgått talar sakliga skäl med styrka emot detta.

De bestämmelser som finns i sådana författningar om personuppgiftsansvar, sökbegränsningar m.m. kommer emellertid att efter hand kunna anpassas för att harmoniera med den nya lagen. Huruvida den nya lagen ska ersätta sådana bestämmelser eller inte får bedömas från fall till fall.

Att det även i fortsättningen kommer att finnas renodlade registerförfattningar utesluter alltså på inget sätt att sådana författningar ”rensas” från dataskyddsbestämmelser varefter författningen bara innehåller de verksamhetsregler m.m. som bör gälla för registret. Sådana bestämmelser som utgör särreglering i förhållande till den av oss föreslagna lagen och som alltjämt anses behövas, skulle då kunna föras in i den till lagen anslutande förordningen. Huruvida en sådan ordning bör tillämpas för ett enskilt register eller om det är mera lämpligt att särregleringen finns kvar i den särskilda registerförfattningen måste dock avgöras i det särskilda fallet. Vi återkommer till detta i avsnitt 19.1.

På motsvarande sätt förhåller det sig beträffande andra typer av författningar som varken är renodlade registerförfattningar eller informationshanteringsförfattningar utan tillhör den kategori författningar som har inslag av bestämmelser om behandling av personuppgifter bland annan slags reglering. En sådan författning är kameraövervakningslagen (2013:416). Ett annat exempel är lagen (2001:99) om officiell statistik med anknytande förordning som innehåller särreglering om behandling av personuppgifter i sådan särskild statistikverksamhet som bedrivs av statistikansvariga myndigheter, t.ex. Försäkringskassan och Centrala studiestödsnämnden.

Däremot är det vår ambition att de registerförfattningar som har karaktär av informationshanteringsförfattningar efter hand avvecklas och ersätts av den nya lagen, eventuellt med viss fortsatt särreglering i anslutande förordning eller, vid behov, i bilaga till lagen.

Den nya lagen bör alltså inte redan genom ikraftträdandet ersätta några befintliga registerförfattningar. För detta krävs anpassningar som kräver en analys och avvägning av vilka behov av särregler det finns på olika områden och på vilken normnivå dessa särregler i så fall bör ges.

För att få en fungerande omställningsprocess och för att på längre sikt öppna för flexibilitet när det gäller utrymme för att, efter en närmare analys, låta viss reglering helt eller delvis kvarstå eller införas helt åtskild från den samlade regleringen bedömer vi alltså att den nya lagen måste göras subsidiär i förhållande till annan särreglering i lag eller förordning med undantag för personuppgiftslagen och personuppgiftsförordningen. Vi föreslår därför att en sådan bestämmelse tas in i lagen.

8.2.4 Vilka slags behandlingar och uppgifter bör omfattas av lagens tillämpningsområde?

Förslag: Lagen ska tillämpas vid sådan behandling av personuppgifter som är helt eller delvis automatiserad. Lagen gäller även för manuell behandling av personuppgifter om uppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier. Tillämpningsområdet motsvarar alltså personuppgiftslagens tillämpningsområde.

En fråga rörande tillämpningsområdet är vilka slags behandlingar som ska omfattas av regleringen. Dataskyddsdirektivet liksom personuppgiftslagen gäller för sådan behandling av personuppgifter som är helt eller delvis automatiserad samt även annan behandling av personuppgifter om uppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier (artikel 2 c och 3.1 i direktivet och 5 § PuL). Man brukar beskriva det sistnämnda med att det syftar på manuella register. Uppgiftsskyddsförordningens tillämpningsområde är i detta hänseende detsamma som dataskyddsdirektivets (artikel 2.1 och 4.4).

Det normala för befintliga informationshanteringsförfattningar är att de i detta avseende har samma tillämpningsområde som personuppgiftslagen. Något skäl till varför den nya lagen skulle avvika från denna ordning kan vi inte se. Vi föreslår därför en bestämmelse med en med dataskyddsdirektivet överensstämmande definition av vad för slags behandling som lagen är tillämplig på.

En annan fråga som ibland regleras i registerförfattningar är om även andra uppgifter än personuppgifter ska omfattas av regleringen.

Med personuppgifter avses all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet (3 § PuL, se även dataskyddsdirektivet artikel 2). Ibland utsträcks en reglering i en registerförfattning till att även avse uppgifter om avlidna (t.ex. patientdatalagen) eller juridiska personer (t.ex. lagen om behandling av uppgifter i Skatteverkets beskattningsverksamhet). Detta har då föranletts av särskilda förhållanden inom de reglerade verksamheterna.

De regler som den nya lagen ska innehålla ska gälla generellt. Det ter sig mot den bakgrunden inte lämpligt att utvidga regleringen till att omfatta andra kategorier av registrerade än vad som följer av den unionsrättsliga dataskyddsregleringen. Förslaget till uppgiftsskyddsförordning innehåller ingen förändring på denna punkt i förhållande till dataskyddsdirektivet. De generella bestämmelserna i lagen bör således endast gälla för behandling av personuppgifter i den mening som avses i 3 § PuL.

Det är en annan sak att det fortsatt på vissa områden kan finnas anledning att låta vissa särbestämmelser omfatta även uppgifter om avlidna personer eller juridiska personer.

8.3 Lagens förhållande till personuppgiftslagen

Som har framgått av avsnitt 7.1.3 anser vi alltså att det inte finns skäl att invänta resultatet av reformarbetet inom EU utan att den nya lagen bör ges en utformning som är förenlig med gällande rätt. Den nya lagen måste därför förhålla sig till personuppgiftslagen. Frågan är på vilket sätt det bör ske.

8.3.1 Bakgrund

Tre regleringsmodeller

Enligt 2 § PuL gäller avvikande bestämmelser i annan lag eller förordning framför personuppgiftslagens bestämmelser. Personuppgiftslagen är således subsidiär i förhållande till andra författningar i lag eller förordning.

Vid dataskyddsdirektivets genomförande förutsattes att det skulle finnas ett fortsatt behov, framför allt inom den offentliga sektorn, av sektorspecifik särreglering i särskilda författningar som skulle gälla före personuppgiftslagen. Traditionen från datalagens tid med en generellt tillämplig lag som kompletteras av specifika registerförfattningar borde därför fortsätta (prop. 1997/98:44 s. 40 f.). Med personuppgiftslagen kom emellertid den lagtekniska konstruktionen för särregleringens förhållande till den generella regleringen i personuppgiftslagen att bli en komplex och omdiskuterad fråga. Olika mer eller mindre parallella lagstiftningsärenden ledde till att det

ganska snart efter personuppgiftslagens införande utformades olikartade konstruktioner. Detta förhållande präglar än i dag registerlagstiftningen och utgör en av delförklaringarna till varför rättsområdet kommit att uppfattas som svårtillgängligt. Tre förekommande varianter eller modeller kan urskiljas, den kompletterande, den hänvisande och den heltäckande modellen.

De flesta registerförfattningar är utformade i enlighet med den kompletterande modellen. Den tekniken kännetecknas av att särregleringen endast kompletterar eller ersätter personuppgiftslagen i frågor som är specifika för de verksamheter som omfattas av särlagstiftningen. Detta innebär att den myndighet som berörs måste tillämpa såväl den särskilda registerförfattningen som personuppgiftslagen vid sin behandling av personuppgifter. Personuppgiftslagen ska alltså tillämpas om inte annat följer av registerförfattningen eller av föreskrifter som meddelats med stöd av registerförfattningen. Detta gäller alldeles oavsett om registerförfattningen i fråga innehåller eller inte innehåller någon bestämmelse som anger vilket förhållande som gäller mellan författningen och personuppgiftslagen. Frågan om en viss bestämmelse innefattar en avvikelse från vad som ska gälla enligt personuppgiftslagen får avgöras med tillämpning av sedvanliga metoder för tolkning av författningar (prop. 1997/98:44 s. 115 f.). Trots att det i teknisk mening alltså inte måste regleras att registerförfattningen och personuppgiftslagen kompletterar varandra på detta sätt innehåller registerförfattningar ofta bestämmelser som ger uttryck för förhållandet till personuppgiftslagen, dvs. det anges på ett eller annat sätt att personuppgiftslagen gäller utöver registerförfattningen.

Den kompletterande modellen, som alltså är den vanligaste, gäller för bl.a. Arbetsförmedlingen, Centrala studiestödsnämnden, Försäkringskassan, Kriminalvården, Skatteverkets skattebrottsenheter, Totalförsvarets rekryteringsmyndighet samt myndigheter inom hälso- och sjukvården och socialtjänsten. I författningar med denna konstruktion brukar det uttryckas särskilt hur lagen förhåller sig till personuppgiftslagen, som regel under en särskild rubrik, exempelvis Förhållandet till personuppgiftslagen eller något liknande, se t.ex. 2 § lagen (2002:546) om behandling av personuppgifter i den arbetsmarknadspolitiska verksamheten, 1 kap. 4 § patientdatalagen (2008:355) och 2 § studiestödsdatalagen (2009:287).

Även i renodlade registerförfattningar förekommer att förhållandet till personuppgiftslagen klargörs genom uttryckliga bestämmelser. I 3 § lagen om receptregister (1996:1156) och i 2 § lagen (2001:558) om vägtrafikregister finns exempelvis uttryckliga bestämmelser av innebörd att personuppgiftslagen gäller utöver författningen i fråga. Lagen (2000:224) om fastighetsregister och handelsregisterlagen (1974:157) utgör exempel på motsatsen.

Enligt den hänvisande modellen anges i registerförfattningen att den gäller i stället för personuppgiftslagen, om inte annat anges i bestämmelser i registerförfattningen som hänvisar till särskilt utpekade bestämmelser i personuppgiftslagen som ska vara tillämpliga även vid behandling av personuppgifter enligt registerförfattningen i fråga. Även vid den hänvisande modellen måste alltså myndigheten tillämpa såväl den särskilda registerförfattningen som personuppgiftslagen vid sin behandling av personuppgifter. Däremot behöver man inte jämföra bestämmelserna i de båda författningarna för att komma fram till vad som gäller. Den hänvisande modellen används bl.a. i de informationshanteringsförfattningar som gäller för behandling av personuppgifter i Skatteverkets beskattnings- och folkbokföringsverksamhet, Kronofogdemyndighetens verksamhet och i Tullverkets verksamhet. Tekniken används även i bl.a. polisdatalagen (2010:361) och i kustbevakningsdatalagen (2012:145) samt föreslås i en ny lag för personuppgiftsbehandlingen i domstolarnas rättskipande och rättsvårdande verksamhet (Ds 2013:10).

Vid registerförfattningar som är konstruerade enligt den heltäckande modellen är personuppgiftslagen över huvud taget inte tillämplig beträffande den behandling av personuppgifter som regleras genom författningen. De bestämmelser i personuppgiftslagen som trots detta ska tillämpas i den aktuella verksamheten upprepas i stället i registerförfattningen, vilket i praktiken innebär ett slags dubbelreglering. Fördelen är att tillämparen inte behöver läsa i två olika lagar – registerförfattningen respektive personuppgiftslagen – för att konstatera vilka bestämmelser som reglerar den aktuella personuppgiftsbehandlingen. Registerförfattningen är således heltäckande i det avseendet att den helt ersätter personuppgiftslagen. Denna modell används i lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst samt i lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse-

och utvecklingsverksamhet. Den heltäckande modellen används också i kameraövervakningslagen (2013:460).

Vissa motivuttalanden rörande regleringsmodell

Man kan fråga sig av vilka skäl det har valts olika lösningar för relationen mellan personuppgiftslagen och den aktuella särregleringen. Något givet svar på den frågan finns dock inte. För- och nackdelar med de olika modellerna har emellertid diskuterats i förarbeten, en diskussion som här kort ska redogöras för.

En av de första informationshanteringsförfattningar som infördes efter personuppgiftslagens ikraftträdande var dåvarande polisdatalagen (1998:622) som utformades i enlighet med den kompletterande modellen. Flera remissinstanser, bl.a. JO, hade i stället förordat en mer fullständig lösning med en inarbetning i polisdatalagen av tillämpliga bestämmelser i personuppgiftslagen. Regeringen avvisade emellertid en sådan lösning och anförde att ett system som upprepar personuppgiftslagens bestämmelser i polisdatalagen och i de övriga registerförfattningar som måste anpassas till personuppgiftslagens bestämmelser skulle bli väldigt tungrott. Regeringen ansåg därför att man borde undvika en dubbelreglering. Däremot framhölls vikten av att behovet av särreglering noga övervägs och att registerlagstiftningen görs så tydlig att det inte råder någon tvekan om vilka regler i personuppgiftslagen som gäller trots särregleringen (prop. 1997/98:97 s. 97).

Registerförfattningsutredningen kom strax därefter att, i sina förslag rörande personuppgiftsbehandlingen inom bl.a. skatte-, exekution- och tullväsendet, föreslå en hänvisande modell där det angavs vilka bestämmelser i personuppgiftslagen som skulle vara tillämpliga. Enligt utredningen fanns ett stort värde i att inte lämna lagtillämparen utan vägledning när det gäller tolkningen av vilka bestämmelser i personuppgiftslagen som är tillämpliga inom de områden som regleras i speciallagarna. Utredningen framhöll att även om detta innebär att det är nödvändigt för lagtillämparen att ha personuppgiftslagen till hands, undanröjs en hel del av det merarbete det innebär för denne att gå igenom lagarna parallellt och jämföra olika bestämmelser (SOU 1999:105 s. 204). Lagrådet fann dock i det aktuella lagstiftningsärendet att lagstiftningstekniken var otillfreds-

ställande. Den var också enligt Lagrådet riskfylld, med hänsyn såväl till svårigheten att överblicka om dataskyddsdirektivet blir till fullo genomfört i registerlagarna som till möjligheten att, vid kommande lagändringar, hänvisningarna till personuppgiftslagen blir felaktiga eller ofullständiga. Tekniken synes ha tillkommit av hänsyn till myndigheternas bekvämlighet men detta syfte skulle enligt Lagrådet lika gärna ha kunnat vinnas genom administrativa anvisningar (prop. 2000/01:33 s. 345). Regeringen valde dock, trots Lagrådets invändningar, att använda den av utredningen föreslagna hänvisande modellen och anförde, utöver de skäl utredningen hade framhållit, att lagen därmed blir överskådlig och tydlig för tillämparen. Den medför också överskådlighet för den enskilde som därigenom lättare kan utnyttja de rättigheter som tillerkänns denne (a. prop. s. 88).

Efter lagstiftningsärendet rörande skatte-, exekution- och tullväsendet utformades i stort sett alla nya informationshanteringsförfattningar enligt den kompletterande modellen, frånsett den för Tullverkets brottsbekämpande verksamhet från år 2005. I olika förarbeten och i utredningsdirektiv uttalade regeringen att de särskilda registerförfattningarna som huvudregel bör gälla utöver personuppgiftslagen och begränsas till att avse frågor som är specifika för den verksamhet som regleras av lagstiftningen (se t.ex. prop. 2008/09:96 s. 30 f. och dir. 2004:95).

Vid valet av den heltäckande modellen för informationshanteringsförfattningarna för Försvarsmaktens underrättelsetjänst respektive Försvarets radioanstalt framhölls som en viktig faktor att dataskyddsdirektivet inte är tillämpligt på den aktuella personuppgiftsbehandlingen. Det fanns således inte något behov av att kunna överblicka om direktivet blivit korrekt genomfört på det aktuella området (prop. 2006/07:46 s. 45).

Genom den nu gällande polisdatalagen kom den hänvisande modellen att på nytt genomföras i en större reform för dataskyddsregleringen inom polisväsendet. Även kustbevakningsdatalagen är utformad enligt den hänvisande modellen. Inte i något av dessa fall framförde Lagrådet några förnyade invändningar. I allt väsentligt anförde regeringen samma skäl för att välja den hänvisande modellen som i samband med lagstiftningsärendet för skatte-, exekution- och tullväsendet (se prop. 2009/10:85 s. 79 f.). Dessutom anfördes att det är av värde att lagar för myndigheter som i allt ökande

omfattning samarbetar är uppbyggda enligt samma lagstiftningsteknik (jfr lagen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet). Liknande argument för en hänvisande lösning anförs i promemorian med förslag till domstolsdatalag (Ds 2013:10 s. 54 f.).

8.3.2 Våra överväganden och förslag

Förslag och bedömning: Lagen ska gälla i stället för personuppgiftslagen. Den ska dock särskilt hänvisa till vissa bestämmelser i personuppgiftslagen som ska tillämpas på motsvarande sätt vid myndigheters behandling av personuppgifter enligt den nya lagen. Sådana hänvisningar ska bl.a. göras till bestämmelserna om definitioner och om förhållandet till offentlighetsprincipen.

Det finns ett antal bestämmelser i personuppgiftslagen som över huvud taget inte är aktuella att tillämpa på myndighetsområdet. Det finns vidare ett antal regler i personuppgiftslagen som visserligen skulle kunna sägas ha relevans även vid myndigheters behandling av personuppgifter men som ändå inte bör vara tillämpliga vid personuppgiftsbehandling enligt den nya lagen. Det gäller bl.a. den s.k. missbruksregeln i 5 a §, bestämmelsen om personuppgiftsbehandling för direkt marknadsföring i 11 § och bestämmelsen om automatiserade beslut i 29 §.

Förhållandet till personuppgiftslagen

Det är väsentligt att den lagtekniska konstruktionen för hur förhållandet mellan den nya lagen och personuppgiftslagen ska regleras blir ändamålsenlig. I det ligger framför allt en ambition att regleringen ska vara tydlig, lätt att tillämpa och inte riskera att ge upphov till osäkerhet. De redovisade modeller som förekommer bland gällande registerförfattningar är, som framgått, alla förenade med vissa nackdelar. Vi har emellertid inte funnit någon ytterligare regleringsteknik som eliminerar samtliga dessa nackdelar. Någon av de nämnda modellerna bör därför väljas.

Vid valet av modell bör beaktas att lagen kommer att ha en mycket brett tillämpningsområde, i vart fall efter hand. Det är

därför ändamålsenligt med en reglering som är så ”självbärande” som möjligt, dvs. som inte i någon större omfattning förutsätter att det ska göras komplicerade analyser av relationen mellan bestämmelser i den nya lagen respektive personuppgiftslagen. Detta skulle kunna sägas tala för att utforma lagen i enlighet med den heltäckande modellen där man alltså inför bestämmelser som motsvarar sådana bestämmelser i personuppgiftslagen som ska vara tillämpliga. En sådan lösning skulle emellertid bli mycket tungrodd och resultera i en omotiverad dubbelreglering. Till detta kommer att den nya lagen inte syftar till en ny implementering av dataskyddsdirektivet på myndighetsområdet utan till att skapa en för myndigheter bättre anpassad reglering avseende de särförhållanden som inte på ett adekvat sätt kunnat tas om hand genom personuppgiftslagens generella reglering. En heltäckande lag torde vidare göra nödvändiga reformer i samband med införandet av den allmänna uppgiftsskyddsförordningen avsevärt mer komplicerade. En heltäckande modell bör därför inte väljas.

Vi instämmer i de invändningar mot den kompletterande modellen som framförts genom åren om att det inte sällan uppstår svårigheter att bedöma vilka bestämmelser i personuppgiftslagen som fortfarande är tillämpliga vid behandling av personuppgifter enligt en informationshanteringsförfattning. Fråga kan t.ex. uppstå huruvida en bestämmelse i författningen helt eller delvis ersätter en viss bestämmelse i personuppgiftslagen eller om den ”bara” kompletterar bestämmelsen som alltså fortfarande skulle kunna vara tillämplig i och för sig. Det är också svårt att bedöma vilka konsekvenser ändringar i personuppgiftslagen får på tillämpningsområdet för registerförfattningar utformade enligt den kompletterande modellen. Ett exempel är införandet av den s.k. missbruksregeln (5 a § PuL). Enligt den bestämmelsen behöver vissa centrala bestämmelser i personuppgiftslagen inte tillämpas vid behandling av personuppgifter i s.k. ostrukturerat material. I förarbetena till missbruksregeln berördes inte vilka konsekvenser den nya bestämmelsen skulle få för då gällande informationshanteringsförfattningar vars tillämpningsområde omfattar personuppgiftsbehandling i både strukturerat och ostrukturerat material. Ofta har dessa särlagar, såvitt kan förstås av deras förarbeten, utformats med den förutsättningen att exempelvis de grundläggande kraven i 9 § PuL alltid ska gälla. Det kan alltså konstateras att den farhåga Lagrådet förde fram rörande den hän-

visande modellen, om att svårigheter kan uppstå genom att hänvisningar blir felaktiga om personuppgiftslagen ändras, har ett slags motsvarighet beträffande vilka konsekvenser ändringar i personuppgiftslagen får för registerförfattningar utformade enligt den kompletterande modellen.

Vi menar att övervägande skäl talar för att den hänvisande modellen är den mest lämpliga lagtekniska konstruktionen beträffande den nya lagens förhållande till personuppgiftslagen. Därigenom blir regleringen tydlig och lättillämpad. Vi menar också att den modellen erfarenhetsmässigt skapar bäst förutsättningar för att undvika att oklara rättslägen uppstår. Vidare bedömer vi att den hänvisande modellen är avgjort bäst lämpad för att möta de förändringar som kan antas komma att behöva ske som ett resultat av ett införande av en unionsrättslig uppgiftsskyddsförordning.

Vi föreslår därför en bestämmelse som innebär att den nya lagen ska gälla i stället för personuppgiftslagen och att det särskilt hänvisas till vissa bestämmelser i personuppgiftslagen som ska tillämpas på motsvarande sätt vid myndigheters behandling av personuppgifter enligt den nya lagen. Anledningen till uttrycket ”på motsvarande sätt” är att flertalet bestämmelser i personuppgiftslagen avser situationer då något görs ”enligt lagen” eller så refereras på annat sätt till ”lagen”. Med lagen avses i dessa bestämmelser personuppgiftslagen. Meningen är emellertid att syftningen, i de fall en hänvisning görs från den nya lagen, ska avse den lagen och inte personuppgiftslagen (jfr prop. 2012/13:163 s. 47 f. och 109).

Nedan gör vi vissa allmänna överväganden rörande vissa bestämmelser som vi föreslår att den nya lagen ska hänvisa till eller som vi föreslår inte ska vara tillämpliga vid behandling av personuppgifter enligt lagen. Beträffande flertalet bestämmelser i personuppgiftslagen kommer det att i kapitel 9–18 närmare behandlas huruvida vi föreslår hänvisningar eller om ersättande bestämmelser innehållande motsvarigheter till bestämmelser i personuppgiftslagen i stället föreslås. I detta kapitel behandlas bara de bestämmelser som rör mer allmänna frågor eller som inte anknyter till något av de följande kapitlen.

Vissa bestämmelser i personuppgiftslagen som bör gälla enligt den nya lagen

I 3 § PuL definieras ett antal begrepp – behandling (av personuppgifter), blockering (av personuppgifter), mottagare, personuppgifter, personuppgiftsansvarig, personuppgiftsbiträde, personuppgiftsombud, den registrerade, samtycke, tillsynsmyndighet, tredjeland och tredje man – som har sin motsvarighet i artikel 2 i dataskyddsdirektivet. I ett flertal fall används motsvarande begrepp i den nya lagen. Dessa bör ges samma innebörd som i personuppgiftslagen. En hänvisning till 3 § bör därför göras.

I 8 § första stycket PuL anges att bestämmelserna i personuppgiftslagen inte ska tillämpas i den utsträckning det skulle inskränka en myndighets skyldighet enligt 2 kap. TF att lämna ut personuppgifter. Detta förhållande följer i och för sig redan av den formella lagkraftens princip, dvs. att grundlag har företräde framför vanlig lag. Det har dock ansetts väsentligt att förtydliga och upplysa om förhållandet mellan den grundlagsstadgade handlingsoffentligheten och dataskyddsdirektivet (prop. 1997/98:44 s. 46). Bestämmelsen är alltså inte avsedd att ha någon materiell betydelse.

I registerförfattningar konstruerade enligt den hänvisande modellen brukar hänvisas till att 8 § PuL ska vara tillämplig. Vi anser oss inte ha anledning att närmare gå in på den tidvis mycket omdiskuterade frågan om offentlighetsprincipens förhållande till dataskyddsdirektivet utan konstaterar bara att den svenske lagstiftaren intagit den positionen att tryckfrihetsförordningen i detta hänseende har företräde framför direktivet. Vi bedömer att en hänvisning till bestämmelsen om förhållandet till handlingsoffentligheten lämpligen bör göras även i den nya lagen.

Vissa bestämmelser i personuppgiftslagen som inte bör gälla enligt den nya lagen

Det finns ett antal bestämmelser i personuppgiftslagen som över huvud taget inte är aktuella att tillämpa på myndighetsområdet.

Bestämmelserna i 4 § om territoriella tillämpningsområdet är ett exempel. Det säger sig självt att svenska myndigheter är etablerade i Sverige.

Undantaget i 6 § för privat behandling av personuppgifter är ett annat exempel på en bestämmelse i personuppgiftslagen som inte är relevant för myndigheter.

Vad därefter gäller 7 § första stycket om förhållandet till tryck- och yttrandefriheten avser detta sådana grundlagsskyddade rättigheter för medborgarna i förhållande till det allmänna som inte är något som tillkommer eller kan åberopas av myndigheter. Någon sådan hänvisning är alltså inte aktuell.

Av 7 § andra stycket följer att vissa bestämmelser i personuppgiftslagen inte ska tillämpas på sådan personuppgiftsbehandling som sker uteslutande för journalistiska ändamål eller konstnärligt eller litterärt skapande. Inom en hel del myndigheter bedrivs onekligen journalistisk verksamhet, t.ex. genom personaltidningar eller utgivande av mer publika facktidningar eller facklitteratur. Även litterärt skapande förekommer. På vissa särskilda myndigheter, såsom t.ex. konsthögskolor, statliga eller kommunala teatrar eller museer bedrivs vidare konstnärligt skapande i betydande omfattning. För att undantagen i andra stycket ska kunna tillämpas krävs emellertid att personuppgiftsbehandlingen uteslutande sker för de angivna syftena. Ett sådant ensidigt syfte torde knappast kunna sägas förekomma i verksamhet som en myndighet ansvarar för. Vi anser därför att det inte bör hänvisas till 7 § andra stycket.

Utöver de nu nämnda bestämmelserna finns några ytterligare bestämmelser i personuppgiftslagen som bör behandlas i detta sammanhang.

En sådan bestämmelse är den s.k. missbruksregeln i 5 a §. Enligt paragrafens första stycke behöver 9, 10, 13–19, 21–26, 28, 33, 34 och 42 §§ PuL inte tillämpas vid behandling av personuppgifter som inte ingår i eller är avsedda att ingå i en samling av personuppgifter som har strukturerats för att påtagligt underlätta sökning efter eller sammanställning av personuppgifter. I andra stycket föreskrivs att sådan behandling som avses i första stycket, dvs. behandling i s.k. ostrukturerat material, inte får utföras om den innebär en kränkning av den registrerades personliga integritet. Myndigheter är inte undantagna från tillämpningsområdet för missbruksregeln. Av förarbetena till bestämmelsen framgår emellertid att den motiverats av helt andra skäl än att underlätta myndigheternas informationshantering.

Till stöd för att göra undantagen enligt 5 a § har lagstiftaren i huvudsak åberopat artikel 13.1 g i dataskyddsdirektivet om möjligheter att göra undantag med hänsyn till skyddet av fri- och rättigheter. Härmed åsyftas framför allt rätten till yttrandefrihet och informationsfrihet, dvs. rättigheter som enligt 2 kap. 1 § RF tillkommer var och en gentemot det allmänna (prop. 2005/06:173 s. 31 f.). Myndigheter kan inte åberopa dessa rättigheter och torde inte ha sådana fri- och rättigheter som avses i artikel 13.1 g dataskyddsdirektivet. Man kan därvid fråga sig om det över huvud taget är förenligt med dataskyddsdirektivet att tillämpa 5 a § på myndighetsområdet. Från rent principiella utgångspunkter vore det vidare klart otillfredsställande om myndigheterna ägnade sig åt personuppgiftsbehandling som för att vara laglig skulle behöva rättfärdigas enbart med stöd av undantagsregeln i 5 a §. Utgångspunkten bör tvärtom vara att dataskyddsdirektivets hanteringsregler ska iakttas. Vi kan inte heller se att missbruksregeln generellt sett fyller något egentligt behov för myndigheternas del, bortsett från att man slipper göra vissa rättsliga bedömningar och analyser som annars skulle krävas. Sådana faktorer uppväger dock inte, menar vi, de tungt vägande principiella skäl som talar mot missbruksregelns tillämplighet hos myndigheterna.

Det kan för övrigt anmärkas att det mesta tyder på att missbruksregeln inte kommer att kunna behållas vid införandet av uppgiftsskyddsförordningen. Att för myndigheternas vidkommande utmönstra missbruksregeln ligger således helt i linje med vårt uppdrag att skapa en reglering som är väl anpassad till den unionsrättsliga dataskyddsreformen.

Någon hänvisning till 5 a § bör alltså inte göras. I senare avsnitt kommer vi att behandla huruvida det i avgränsade frågor behövs något motsvarande undantag för behandling av personuppgifter som sker i ostrukturerat material.

I 11 § anges att personuppgifter inte får behandlas för ändamål som rör direkt marknadsföring, om den registrerade hos den personuppgiftsansvarige skriftligen har anmält att han eller hon motsätter sig sådan behandling.

Myndigheter ägnar sig inte åt direkt marknadsföring. Däremot förekommer att personuppgifter lämnas ut från en myndighet till en mottagare som avser använda uppgifterna för direkt marknadsföring. En del myndigheter har vidare rätt att i det syftet sälja per-

sonuppgifter. Det förekommer att myndigheter för en förteckning över anmälningar från enskilda registrerade som motsatt sig användning för marknadsföringssyfte. Någon möjlighet för myndigheten att med stöd av 11 § vägra lämna ut personuppgifter rörande registrerade som gjort en anmälan till myndigheten enligt 11 § torde i praktiken inte finnas när den som begär ut uppgifterna åberopar 2 kap. TF till stöd för sin begäran om att få ut uppgifterna. Däremot kan sekretess eventuellt föreligga enligt 21 kap. 7 § OSL (beträffande denna paragraf, se avsnitt 11.2). Någon hänvisning till 11 § PuL bör därför inte göras. Det innebär dock, som vi ser det, självfallet inte något hinder mot att myndigheter fortsätter att tillhandahålla blanketter och särskild information om möjligheten för registrerade att anmäla att de motsätter sig användning för marknadsföringsändamål och att myndigheten fortsätter föra en förteckning över sådana anmälningar.

Slutligen ska beröras 29 § PuL om automatiserade beslut. I den paragrafens första stycke föreskrivs att om ett beslut som har rättsliga följder för en fysisk person eller annars har märkbara verkningar för den fysiska personen, grundas enbart på automatiserad behandling av sådana personuppgifter som är avsedda att bedöma egenskaper hos personen, ska den som berörs av beslutet ha möjlighet att på begäran få detta omprövat av någon person. Andra stycket handlar om information som ska lämnas vid beslut som avses i första stycket.

Automatiserat beslutsfattande förekommer i den offentliga förvaltningen. Däremot torde det inte förekomma det slags automatiserade beslut som avses i 29 § PuL. I den utsträckning sådana beslut ändå förekommer, följer av grundläggande rättssäkerhetsprinciper inom förvaltningen att besluten kan omprövas respektive överklagas. Vi bedömer att det inte torde förekomma automatiserade beslut av det slag som avses i 29 § som inte går att få omprövade av en befattningshavare. Mot den bakgrunden behövs ingen hänvisning till 29 §.

9 Tillåten behandling

9.1 Hur bestäms vad som är en statlig eller kommunal myndighets verksamhet?

Regeringsformen innehåller de grundläggande bestämmelserna om den svenska förvaltningsorganisationen. Enligt 1 kap. 1 § RF utgår all offentlig makt i Sverige från folket. Den förverkligas genom ett representativt och parlamentariskt statsskick och genom kommunal självstyrelse. Vidare anges att den offentliga makten utövas under lagarna. Därigenom slås fast principen om all maktutövnings lagbundenhet, legalitetsprincipen. Den gäller inte bara domstolar och förvaltningsmyndigheter utan även riksdag och regering. På det kommunala området gäller den i lika hög grad som på det statliga (Holmberg m.fl., kommentaren till 1 kap. 1 § RF).

I 1 kap. 4 § RF föreskrivs att riksdagen är folkets främsta företrädare. Riksdagen stiftar lag, beslutar om skatt till staten och bestämmer hur statens medel ska användas. Riksdagen granskar rikets styrelse och förvaltning.

Enligt 1 kap. 6 § RF är det regeringen som styr riket. Regeringen är ansvarig inför riksdagen. Av 1 kap. 8 § RF framgår att det för rättskipningen finns domstolar och för den offentliga förvaltningen statliga och kommunala förvaltningsmyndigheter.

I 8 kap. RF finns bestämmelser om vilka föreskrifter som meddelas genom lag, dvs. genom beslut av riksdagen, genom förordning av regeringen och av andra myndigheter efter bemyndigande av riksdagen eller regeringen. Enligt 8 kap. 2 § första stycket 3 meddelas föreskrifter om grunderna för kommunernas organisation och verksamhetsformer och för den kommunala beskattningen samt kommunernas befogenheter i övrigt och deras åligganden genom lag.

Ytterligare grundläggande bestämmelser om den statliga förvaltningen finns i 12 kap. RF. Av 1 § följer att Justitiekanslern och

andra statliga förvaltningsmyndigheter, som inte enligt regeringsformen eller annan lag är myndigheter under riksdagen, lyder under regeringen.

I 12 kap. 2 och 3 §§ finns bestämmelser om den statliga förvaltningens självständighet. Enligt 2 § får ingen myndighet, inte heller riksdagen eller en kommuns beslutande organ, bestämma hur en förvaltningsmyndighet i ett särskilt fall ska besluta i ett ärende som rör myndighetsutövning mot en enskild eller mot en kommun eller som rör tillämpningen av lag. I 3 § föreskrivs att förvaltningsuppgifter inte får fullgöras av riksdagen i vidare mån än vad som följer av grundlag eller riksdagsordningen.

Enligt 12 kap. 4 § RF kan förvaltningsuppgifter överlämnas åt kommuner. Denna föreskrift innebär endast en erinran om vad som ändå gäller på grund av 1 kap. 8 § och 8 kap. 2 § första stycket 3 (Holmberg m.fl., kommentaren till 12 kap. 4 § RF).

I 14 kap. finns bestämmelser om kommunerna. Enligt 1 § utövas beslutanderätten i kommunerna av valda församlingar. I 2 § föreskrivs att kommunerna sköter lokala och regionala angelägenheter av allmänt intresse på den kommunala självstyrelsens grund. Närmare bestämmelser om detta finns i lag. På samma grund sköter kommunerna även de övriga angelägenheter som bestäms i lag.

Närmare om de statliga myndigheterna

I den mån statliga myndigheters verksamhet inte är lagreglerad ankommer det på regeringen att bestämma om detta. Som framgått följer av 12 kap. 1 § RF att huvudregeln är att de statliga myndigheterna lyder under regeringen. Förvaltningen har således att förverkliga regeringens politik. Den har en lydnadsrelation till regeringen, inte till riksdagen eller medborgarna och inte heller till ett enskilt statsråd. Det är också regeringen som lämnar uppdragen till förvaltningen. Annorlunda uttryckt kan man säga att regeringen delegerar en del av sitt ansvar till myndigheterna. Förutom på det område där förvaltningens lydnadsplikt gentemot regeringen enligt 12 kap. 2 § RF inte gäller, dvs. då det är fråga om ärenden som rör myndighetsutövning mot enskilda eller mot kommuner eller när det gäller tillämpning av lag, är alltså regeringen inför riksdagen ytterst ansvarig för allt som myndigheterna gör (SOU 2007:75

s. 40). När det gäller samspelet mellan regeringen och myndigheterna har det ansetts viktigt att betona att förvaltningen också har en legitim rätt att hävda sina ståndpunkter och att den också förutsätts stå för olika värden (a. bet. s. 41).

Regeringen lämnar sina uppdrag till förvaltningen på olika sätt. Det kan ske genom att regeringen inom ramen för sin kompetens enligt 8 kap. RF utfärdar föreskrifter för förvaltningen. I den mån en myndighets uppgifter inte har fastställts i en lag, lägger regeringen fast myndighetens uppgifter i en förordning med instruktion för myndigheten. Regeringen anvisar vidare medel för myndigheternas verksamhet inom ramen för riksdagens budgetbeslut enligt bestämmelserna i 9 kap. RF. I regleringsbrev till de statliga myndigheterna utfärdar regeringen regler om hur dessa medel får användas av myndigheterna. Även regleringsbreven kan innehålla uppdrag från regeringen till myndigheten i fråga. Uppdrag till myndigheterna kan också ges i särskilda beslut.

Regeringen har bedömt att det för varje förvaltningsmyndighet – kommittéer och särskilda utredare undantagna – bör finnas en förordning med instruktion för myndigheten (prop. 2009/10:175 s. 111 f.). En sådan förordning kan vara gemensam för flera myndigheter med liknande verksamhet eller för flera myndigheter inom samma förvaltningsområde. I instruktionen bör myndighetens ansvarsområde, uppgifter, ledningsform och andra för myndigheten specifika förhållanden regleras. Instruktionen bör enligt regeringen vara det grundläggande instrumentet i regeringens styrning av myndigheterna. Uppgifter som är tidsbegränsade eller som kan förväntas att ändras inom en närmare framtid liksom uppgifter eller uppdrag där regeringen ser behov av att vara utförlig i beskrivningen är exempel på sådant som vanligen däremot inte regleras i instruktionen utan i annat beslut. Sedan 2009 gäller vidare att myndigheterna i enlighet med förordningen (2000:605) om årsredovisning och budgetunderlag i sin årsredovisning ska redovisa och kommentera verksamhetens resultat i förhållande till de uppgifter som framgår av myndighetens instruktion och till vad regeringen, i förekommande fall, har angett i regleringsbrev eller i något annat beslut. Detta innebär att revisionen fortsättningsvis som regel görs med utgångspunkt i myndigheternas instruktion.

Regeringens åtgärder för att lyfta fram myndigheters instruktion som basen för den löpande styrningen och återrapporteringen

av respektive myndighets verksamhet syftade till att öka inslaget av långsiktighet i styrningen av myndigheterna och därmed skapa en mer ändamålsenlig styrning (skr. 2013/14:155 s. 71). Regeringen har genomfört ett omfattande arbete med att se över merparten av alla instruktioner och regleringsbrev i syfte att renodla användningen av dessa styrinstrument, där instruktionen alltså är det huvudsakliga styrinstrumentet. Detta arbete har lett till att regeringens beskrivning av myndigheternas ordinarie verksamhet har minskat väsentligt i regleringsbreven samtidigt som den ökat i myndighetsinstruktionerna under åren 2008–2012 (2012/13:KU10 s. 88 och 98 f.).

Närmare om de kommunala myndigheterna

Enligt 2 kap. 1 § KL får kommuner och landsting själva ha hand om sådana angelägenheter av allmänt intresse som har anknytning till kommunens eller landstingets område eller deras medlemmar och som inte ska handhas av enbart staten, en annan kommun, ett annat landsting eller någon annan. Paragrafen innehåller den grundläggande bestämmelsen om kommunernas och landstingens allmänna kompetens, alltså vad de frivilligt får ägna sig åt. Allmänintresset är det ledande motivet för kommunal verksamhet (Lindquist/Losman, Kommunallagen, 14:e uppl., 2013, s. 22 f). För att en angelägenhet ska kunna betecknas som kommunal måste den i någon mening knyta an till kommunens eller landstingets geografiska område eller till medlemmarna. Paragrafen ger därmed uttryck för den s.k. lokaliseringsprincipen. Till områdena för kommuners och landstings allmänna kompetens hör bl.a. elförsörjningen, idrotts- och fritidsanläggningar, folkbildning och kulturverksamhet samt bostadsbyggande. Verksamhet som utgör frivilliga åtaganden för kommunerna beslutas av kommunerna själva.

I 2 kap. 4 § KL hänvisas till att det finns särskilda föreskrifter om kommunernas och landstingens befogenheter och skyldigheter på vissa områden. Sådan speciallagstiftning innebär utvidgningar eller undantag i förhållande till de allmänna principerna för kommunal verksamhet och tar över reglerna i kommunallagen. Särskilda föreskrifter finns bl.a. i lagen (2009:47) om vissa kommunala befogenheter, den s.k. befogenhetslagen. Den reglerar i flera hänseenden

kompetensgränsen mellan stat och kommun. Med särskilda föreskrifter avses också speciallagar som ålägger kommuner och landsting att bedriva eller sörja för vissa verksamheter och fullgöra olika uppgifter. För kommunerna gäller det exempelvis förskola, skola, socialtjänst, äldreomsorg, stöd och service till vissa funktionshindrade, kommunal hälso- och sjukvård, kollektivtrafik, färdtjänst, plan- och byggväsende, räddningstjänst, renhållning/avfallshantering, lokal miljötillsyn och livsmedelskontroll, vattenförsörjning och avlopp, bostadsförsörjningsansvar, överförmyndarverksamhet och bibliotek. Obligatoriska uppgifter för landstingen är bl.a. hälso- och sjukvård, tandvård, smittskydd och kollektivtrafik. Ekonomiskt sett utgör kommunernas och landstingens obligatoriska verksamheter den absolut största delen av deras verksamhet.

I 3 kap. KL finns bestämmelser om kommunernas och landstingens organisation och verksamhetsformer. Enligt 1 § ska det i varje kommun eller landsting finnas en beslutande församling; kommunalfullmäktige eller landstingsfullmäktige. I 2 § föreskrivs att fullmäktige i en kommun eller ett landsting ska tillsätta en styrelse. Vidare sägs i 3 § att fullmäktige ska tillsätta de nämnder som utöver styrelsen behövs för att fullgöra kommunens eller landstingens uppgifter enligt särskilda författningar och för verksamheten i övrigt. Uppgifterna enligt 3 § får också fullgöras genom en för kommuner och landsting gemensam nämnd (3 a §). I 9 och 10 §§ finns bestämmelser om i vilka ärenden som enbart fullmäktige är behörig att besluta respektive när fullmäktige kan uppdra åt en nämnd att besluta i dess ställe. I 6 kap. 33–38 §§ KL finns föreskrifter om delegering av beslutanderätt i ärenden inom en nämnds verksamhetsområde.

Enligt 3 kap. 13 § KL har nämnderna en egen beslutanderätt, förutom i de frågor som fullmäktige delegerat till dem, dels i fråga om den egna förvaltningen, dvs. vardagliga beslut i den löpande verksamheten, dels i frågor som de enligt lag eller annan författning ska handha.

I detta sammanhang kan också nämnas att det genom föreskrifter i 3 kap. 16 § andra stycket KL ges möjlighet för en kommun eller ett landsting att, under vissa förutsättningar, lämna över vården av en kommunal angelägenhet till ett privaträttsligt subjekt.

9.2 När får myndigheter behandla personuppgifter?

9.2.1 Allmänna dataskyddsrättsliga regler

Dataskyddsdirektivet

Kapitel II i dataskyddsdirektivet innehåller allmänna bestämmelser om när personuppgifter får behandlas. Medlemsstaterna ska inom de begränsningar som bestämmelserna i artiklarna 6–21 innebär, precisera på vilka villkor behandling av personuppgifter är tillåten (artikel 5). Kapitlet är indelat i nio underavdelningar. Avdelning I – Principer om uppgifternas kvalitet – innehåller artikel 6. Avdelning II – Principer som gör att uppgiftsbehandling kan tillåtas – innehåller artikel 7. Dessa artiklar ska redovisas mer ingående i det följande. Övriga avdelningar innehåller bestämmelser om bl.a. särskilda behandlingskategorier (artikel 8–9), informationsplikt m.m. (artikel 10–12), möjligheter till undantag och begränsningar (artikel 13), den registrerades rätt att göra invändningar (artikel 14–15), sekretess och säkerhet (16–17) samt anmälningsplikt till tillsynsmyndighet m.m. (artikel 18–21).

Enligt artikel 6.1 dataskyddsdirektivet ska medlemsstaterna föreskriva att personuppgifter

a. ska behandlas på ett korrekt och lagligt sätt,

b. ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål; senare behandling får inte ske på ett sätt som är oförenligt med dessa ändamål. Senare behandling av uppgifter för historiska, statistiska eller vetenskapliga ändamål ska inte anses oförenlig med dessa ändamål förutsatt att medlemsstaterna beslutar om lämpliga skyddsåtgärder,

c. ska vara adekvata och relevanta och inte får omfatta mer än vad som är nödvändigt med hänsyn till de ändamål för vilka de har samlats in och för vilka de senare behandlas,

d. ska vara riktiga och, om nödvändigt, aktuella. Alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga eller ofullständiga i förhållande till de ändamål för vilka de samlades in eller för vilka de senare behandlas, utplånas eller rättas,

e. förvaras på ett sätt som förhindrar identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka uppgifterna samlades in eller för vilka de senare behandlades. Medlemsstaterna ska vidta lämpliga skyddsåtgärder för de personuppgifter som lagras under längre perioder för historiska, statistiska eller vetenskapliga ändamål.

Enligt artikel 6.2. åligger det den registeransvarige att säkerställa att punkten 1 efterlevs.

I artikel 7 anges att medlemsstaterna ska föreskriva att personuppgifter får behandlas endast om

a. den registrerade otvetydigt har lämnat sitt samtycke, eller

b. behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås, eller

c. behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den registeransvarige, eller

d. behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade, eller

e. behandlingen är nödvändig för att utföra en arbetsuppgift av allmänt intresse eller som är ett led i myndighetsutövning som utförs av den registeransvarige eller tredje man till vilken uppgifterna har lämnats ut, eller

f. behandlingen är nödvändig för ändamål som rör berättigade intressen hos den registeransvarige eller hos den eller de tredje män till vilka uppgifterna har lämnats ut, utom när sådana intressen uppvägs av den registrerades intressen eller dennes grundläggande fri- och rättigheter som kräver skydd under artikel 1.1.

Artiklarna 6 och 7 kan sägas bilda den yttre ramen för hur och när behandling av personuppgifter alls får ske. De rättsliga grunderna i artikel 7 är en uttömmande uppräkning av de situationer när en behandling av personuppgifter kan anses vara tillåten. Får uppgifterna behandlas enligt någon av de rättsliga grunderna i artikel 7, måste emellertid också kraven i artikel 6 följas. Bestämmelserna är alltså kumulativa och utgör de allmänna förutsättningarna för tillåten personuppgiftsbehandling enligt dataskyddsdirektivet. För särskilda

uppgiftskategorier, överföring till tredjeland m.m. finns ytterligare begränsningar.

Från de grundläggande principerna i artikel 6.1 får medlemsstaterna genom lagstiftning begränsa omfattningen av de skyldigheter och rättigheter som anges i artikel 6.1 då det är nödvändigt med hänsyn till vissa specifika intressen som anges i artikel 13.1, bl.a. a) statens säkerhet, b) försvaret, c) allmän säkerhet, e) ett viktigt ekonomiskt eller finansiellt intresse hos unionen eller en medlemsstat och g) skyddet av den registrerades eller andras fri- och rättigheter. I övrigt finns inga bestämmelser i dataskyddsdirektivet som medger medlemsstaterna att föreskriva undantag eller begränsningar i förhållande till artikel 6.

Vad gäller artikel 7 finns inget motsvarande utrymme för undantag genom nationell lagstiftning. EU-domstolen har uttalat att medlemsstaterna, enligt artikel 5, varken får foga ytterligare principer för tillåtligheten av behandlingen av personuppgifter till dem som nämns i artikel 7 eller föreskriva ytterligare villkor som påverkar räckvidden av artikelns sex principer (dom den 24 november 2011 i förenade målen C-468/10 och C-469/10, ASNEF och FECEMED punkt 32 och 36).

Personuppgiftslagen

Artiklarna 6 och 7 i dataskyddsdirektivet har genomförts i svensk rätt i princip ordagrant genom 9 och 10 §§ PuL. När myndigheter, liksom enskilda, behandlar personuppgifter måste det således ske dels i enlighet med vissa grundläggande krav på behandlingen som föreskrivs i 9 § PuL, dels måste behandlingen kunna hänföras till något av de i 10 § uppräknade fall då det över huvud taget är tillåtet att behandla personuppgifter. De båda bestämmelserna är alltså, liksom motsvarigheterna i dataskyddsdirektivet, kumulativa. Avser behandlingen känsliga personuppgifter eller personnummer eller samordningsnummer finns därutöver ytterligare restriktioner vilka gäller också för myndigheter, se 13–16, 18–19 och 22 §§ PuL.

Om personuppgifter behandlas på så sätt att de inte ingår i eller är avsedda att ingå i en samling av personuppgifter som har strukturerats för att påtagligt underlätta sökning efter eller sammanställning av personuppgifter, dvs. behandling i s.k. ostrukturerat

material, gäller ett flertal undantag från personuppgiftslagens hanteringsregler, däribland 9, 10 och 13 §§ PuL. Detta följer av den s.k. missbruksregeln i 5 a § enligt vilken bestämmelserna i vissa uppräknade paragrafer inte behöver följas vid behandling av personuppgifter i s.k. ostrukturerat material under förutsättning att behandlingen inte innebär en kränkning av den registrerades personliga integritet. Missbruksregeln, som infördes genom 2006 års ändringar i personuppgiftslagen (prop. 2005/06:173), är fakultativ, inget hindrar att hanteringsreglerna ändå tillämpas.

Närmare om de grundläggande kraven

I 9 § PuL anges alltså de grundläggande krav på behandlingen av personuppgifter som alltid måste vara uppfyllda när personuppgifter behandlas, även i en myndighets verksamhet, i den mån inte missbruksregeln kan tillämpas. Det är den personuppgiftsansvarige som ansvarar för att de grundläggande kraven är uppfyllda. Det gäller även om den faktiska personuppgiftsbehandlingen sker hos ett personuppgiftsbiträde och oavsett om biträdet är en myndighet eller en enskild aktör. Den registrerade anses inte kunna med rättslig verkan ge sitt samtycke till att personuppgifter om honom eller henne behandlas i strid med paragrafen (Öman/Lindblom, s. 194).

Bestämmelserna i 9 § PuL är avsedda att ha samma innebörd som bestämmelserna i artikel 6 i dataskyddsdirektivet. I 9 § första stycket formuleras kraven uppdelade i följande punkter. Den personuppgiftsansvarige ska se till att

a. personuppgifter behandlas bara om det är lagligt,

b. personuppgifter alltid behandlas på ett korrekt sätt och i enlighet med god sed,

c. personuppgifter samlas in bara för särskilda, uttryckligt angivna och berättigade ändamål,

d. personuppgifter inte behandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in,

e. de personuppgifter som behandlas är adekvata och relevanta i förhållande till ändamålen med behandlingen,

f. inte fler personuppgifter behandlas än som är nödvändigt med hänsyn till ändamålen med behandlingen,

g. de personuppgifter som behandlas är riktiga och, om det är nödvändigt, aktuella,

h. alla rimliga åtgärder vidtas för att rätta, blockera eller utplåna sådana personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålen med behandlingen, och

i. personuppgifter inte bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen.

Punkterna a och b om att personuppgifter får behandlas bara om det är lagligt och korrekt syftar bl.a. på att behandlingen måste kunna hänföras till de rättsliga grunder för behandlingen som anges i 10 § PuL och inte heller i övrigt strider mot någon bestämmelse i personuppgiftslagen eller anknytande föreskrifter. Ordalydelsen utesluter i och för sig inte att annan lagstiftning också åsyftas. Enligt uttalanden i doktrinen kan det framgå av annan lagstiftning, t.ex. brottsbalken eller marknadsföringslagen, när det är olagligt att behandla personuppgifter (Öman/Lindblom, s. 195). Den frågan kan dock ställas vad som egentligen avses med lagligheten som ett grundkrav enligt personuppgiftslagen. Inte minst när det gäller myndigheters behandling av personuppgifter finns en mycket stor mängd författningar utöver personuppgiftslagen som är styrande för informationshanteringen och vars lagenliga efterföljande berörd personuppgiftsansvarig myndighet har ett övergripande ansvar för, oavsett personuppgiftsansvaret. Som exempel kan nämnas reglerna om användningen av hemliga tvångsmedel i 27 kap. RB som utgör en förfaranderegelering för hemlig inhämtning av information, vilken givetvis kan innefatta personuppgifter. Det kan te sig naturligt att läsa 9 § första stycket a PuL på så sätt att en hantering av upptagningar från hemliga tvångsmedel som strider mot rättegångsbalkens krav också skulle vara i strid mot personuppgiftslagens grundläggande krav på att personuppgifter bara får behandlas om det är lagligt. Likaså skulle en behandling av personuppgifter som strider mot något förbud mot att röja en sekretessbelagd personuppgift kunna anses olaglig i den mening som avses i 9 § första stycket a PuL.

Datalagskommittén ansåg för sin del att det är osäkert om dataskyddsdirektivets krav i artikel 6.1 a på att medlemsstaterna ska föreskriva att personuppgifter ska behandlas på ett korrekt och lagligt sätt har någon självständig betydelse. Punkterna a om laglighet och b om korrekthet togs dock med bland de grundläggande kraven i 9 § PuL för säkerhets och fullständighets skull (SOU 1997:39 s. 350). Detta kommenterades inte i propositionen till personuppgiftslagen (prop. 1997/98:44). Det förefaller således inte ha funnits någon klar uppfattning hos den svenska lagstiftaren om vad som egentligen åsyftas med kravet enligt 9 § första stycket a om att personuppgifter ska behandlas lagligt och vilken konsekvensen blir i dataskyddsrättsligt hänseende om t.ex. en myndighet behandlar personuppgifter i strid mot någon bestämmelse i en annan författning än personuppgiftslagen. Detta kan i sin tur ha betydelse för frågan om räckvidden av det skadeståndssanktionerade personuppgiftsansvaret enligt 48 § PuL, dvs. skyldigheten att betala skadestånd för en kränkning av den registrerades personliga integritet orsakad av en personuppgiftsbehandling i strid med personuppgiftslagen. I vilken mån en sådan skyldighet kan uppstå på grund av att en personuppgiftsbehandling t.ex. strider mot rättegångsbalken och därför inte är laglig även om någon annan bestämmelse i personuppgiftslagen inte överträtts förefaller oklart.

Punkterna c och d anger att personuppgifter får samlas in bara för särskilda, uttryckligt angivna och berättigade ändamål samt att redan insamlade personuppgifter inte får användas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in, den s.k. finalitetsprincipen. Finalitetsprincipen är en allmän dataskyddsrättslig princip som getts en uttrycklig och central roll i dataskyddsdirektivet och därmed även i personuppgiftslagen, bl.a. genom att finalitetsprincipen konkretiserats till att vara en av de hanteringsregler som den personuppgiftsansvarige ska vara ålagd att följa. Att bestämningen av ändamålet eller ändamålen för insamling av personuppgifter sker på ett korrekt sätt i enlighet med punkten c har emellertid betydelse inte bara för vilka efterföljande behandlingar som får ske utan även för de återstående grundläggande kraven i 9 § första stycket. Utan särskilda och uttryckligt angivna ändamål går det knappast att bedöma huruvida personuppgifter är adekvata, relevanta och inte för många eller lagras för länge osv. Detta därför att sådana bedömningar alltid ska ske i

förhållande till det eller de ändamål som personuppgifterna behandlas för. Ändamålsbestämning och finalitetsprincipen m.m. kommer att behandlas mer ingående nedan i avsnitt 9.2.3.

När det gäller punkten i om hur länge personuppgifter får bevaras har den bestämmelsen en tämligen begränsad räckvidd på myndigheternas område eftersom den inte gäller i den mån den inkräktar på myndigheters skyldigheter enligt arkivlagstiftningen att bevara allmänna handlingar, 8 § andra stycket PuL. Däremot gäller punkten i för personuppgifter som ingår i upptagningar som inte utgör allmänna handlingar.

När behandling av personuppgifter är tillåten

Bestämmelserna i 10 § PuL innehåller – liksom artikel 7 i dataskyddsdirektivet – en uttömmande uppräkning av de fall då personuppgifter alls får behandlas. Faller en myndighets personuppgiftsbehandling inte in under någon av de rättsliga grunder som anges i 10 § är den alltså otillåten. Det spelar därvid ingen roll om det handlar om personuppgifter som direkt pekar ut en registrerad person eller om det handlar om t.ex. s.k. pseudonymiserade uppgifter eller uppgifter som annars endast indirekt kan härledas till den registrerade personen. Det spelar heller ingen roll om det handlar om insamling av personuppgifter för ett visst ändamål eller behandling av redan insamlade uppgifter för ett nytt ändamål. Även om det nya ändamålet inte är oförenligt med det ursprungliga ändmålet och därför uppfyller det grundläggande kravet i 9 § första stycket d, måste den nya behandlingen dessutom omfattas av någon av grunderna i 10 §.

Enligt 10 § PuL är huvudregeln att personuppgifter får behandlas om den registrerade, dvs. den som en personuppgift avser, har lämnat sitt samtycke till behandlingen. Med samtycke avses enligt 3 § PuL varje slag av frivillig, särskild och otvetydig viljeyttring genom vilken den registrerade, efter att ha fått information, godtar behandling av personuppgifter som rör honom eller henne. Behandling får också ske om personuppgiftsbehandlingen är nödvändig för att

a. ett avtal med den registrerade ska kunna fullgöras eller åtgärder som den registrerade begärt ska kunna vidtas innan ett avtal träffas,

b. den personuppgiftsansvarige ska kunna fullgöra en rättslig skyldighet,

c. vitala intressen för den registrerade ska kunna skyddas,

d. en arbetsuppgift av allmänt intresse ska kunna utföras,

e. den personuppgiftsansvarige eller en tredje man till vilken personuppgifter lämnas ut ska kunna utföra en arbetsuppgift i samband med myndighetsutövning, eller

f. ett ändamål som rör ett berättigat intresse hos den personuppgiftsansvarige eller hos en sådan tredje man till vilken personuppgifterna lämnas ut ska kunna tillgodoses, om detta intresse väger tyngre än den registrerades intresse av skydd mot kränkning av den personliga integriteten.

Det kan knappast sägas gälla några skarpa gränser mellan de rättsliga grunderna i 10 a–e § utan de kan vara överlappande på det sättet att en situation faller in under mer än en punkt. Det är dock i och för sig alltid tillräckligt att en behandling faller in under i vart fall en punkt. Det är alltså fråga om alternativa grunder för behandling.

För myndigheter torde framför allt punkterna b, d och e omfatta sådan personuppgiftsbehandling som behövs i myndigheternas verksamheter. Som redan har framhållits torde t.ex. en stor del av den behandling som utförs inom den offentliga sektorn vara tillåten med stöd av punkten e, i vart fall när det gäller en myndighets egentliga verksamhet (Öman/Lindblom, s. 239). Det är mer tveksamt om bestämmelsen omfattar behandling som äger rum inom en myndighets interna administration och som exempelvis rör personalfrågor. Sådan behandling kan emellertid vara tillåten enligt någon av de andra punkterna som räknas upp i 10 §. Punkten a om behandling i samband med avtal torde t.ex. kunna aktualiseras hos en personuppgiftsansvarig myndighet när den agerar på det civilrättsliga området t.ex. i samband med anställningsförhållanden eller vid köp av varor eller tjänster. Punkten c om behandling för att skydda den registrerades vitala intressen torde också kunna aktualiseras hos vissa myndigheter. I litteraturen har nämnts som exempel situationer i samband med tvångsvård eller vård av medvetslösa eller i räddningstjänsten (Öman/Lindblom, s. 236).

I punkten f finns vidare ett slags generalklausul som medger behandling efter en intresseavvägning. För myndigheters del kan konstateras att en behandling av personuppgifter som bedöms tillåten efter den intresseavvägning som ska göras enligt f också torde vara tillåten enligt något av fallen i a–e och i vart fall enligt d, dvs. att en arbetsuppgift av allmänt intresse ska kunna utföras. Punkten f torde därmed normalt sett inte ha så stor självständig relevans vid myndigheters behandling av personuppgifter. Det har dock förekommit att punkten f ansetts tillämplig vid myndigheters behandling av personuppgifter. Exempelvis har olika myndigheters publicering av personuppgifter på internet prövats utifrån en intresseavvägning enligt 10 § f PuL (Datainspektionens beslut 2004-09-08, dnr 454-2004 och Justitiekanslerns beslut 2007-09-26, dnr 3497-06-40). Högsta förvaltningsdomstolen har vidare i ett fall rörande en kommuns behandling av gymnasieelevers fingeravtryck prövat förutsättningarna för behandling genom en intresseavvägning enligt punkten f (RÅ 2008 ref. 83).

Innebörden av det nödvändighetsrekvisit som föreskrivs för behandling oberoende av samtycke enligt punkterna a–f kan inte sägas vara helt klar. Rekvisitet innebär emellertid inte att det ska vara faktiskt omöjligt att utföra en arbetsuppgift utan sådan automatiserad behandling av personuppgifter som omfattas av personuppgiftslagen. Enligt Datalagskommittén är nödvändighetsrekvisitet i detta avseende inte uppfyllt om arbetsuppgiften kan utföras nästan lika enkelt eller billigt utan behandling av personuppgifter (SOU 1997:39 s. 359). Domstolsdatautredningen uttalade som sin mening att det sannolikt räcker med att det innebär en påtaglig förenkling för den personuppgiftsansvarige att personuppgifter behandlas på automatiserad väg (SOU 2001:100 s. 90).

Sedan dessa uttalanden gjordes har emellertid EU-domstolen gjort vissa uttalanden om nödvändighetsrekvisitet i artikel 7 i dom den 16 december 2008 i mål C-524/06, Huber. Målet rörde bl.a. tolkningen av artikel 7 e – om behandling som är nödvändig för att utföra en arbetsuppgift av allmänt intresse eller som ett led i myndighetsutövning – i samband med en förbundsstatlig tysk myndighets centrala utlänningsregister. Domstolen uttalade att begreppet nödvändighet, såsom det följer av artikel 7 e, inte kan förstås olika från medlemsstat till medlemsstat utan att det är ett självständigt gemenskapsrättsligt begrepp. Det konstaterandet gjordes med beakt-

ande av målet enligt artikel 1.1 i direktivet att göra skyddsnivån likvärdig i alla medlemsstater och att syftet med artikel 7 e är att begränsa ett av de fall i vilket behandling av personuppgifter tillåts (punkt 52). I det aktuella fallet gjorde domstolen bedömningen att nödvändighetsrekvisitet var uppfyllt och behandlingen därmed tillåten om registret a) för det första endast innehöll uppgifter som var nödvändiga för myndighetens rättsliga hantering i ett visst avseende och b) för det andra om den centrala registerföringen medgav en mer effektiv hantering jämfört med om aktuella myndigheter i stället skulle behöva vända sig till varje kommunalt register där motsvarande uppgifter fanns. Nödvändighetsrekvisitet var dock inte uppfyllt såvitt avsåg personuppgifter som behövdes för statistiska ändamål, eftersom det bedömdes räcka med anonyma uppgifter (punkt 58–68).

Något nödvändighetsrekvisit gäller alltså inte enligt 10 § PuL vid behandling som sker med den registrerades samtycke. Oavsett på vilken grund en behandling är tillåten enligt 10 § måste emellertid de grundläggande kraven enligt 9 § följas, t.ex. att inte fler personuppgifter behandlas än vad som behövs för ändamålen m.m.

Bestämmelserna i 10 § PuL om grund för behandlingen hör till det slag av hanteringsregler som inte behöver tillämpas om missbruksregeln i 5 a § gäller, dvs. vid behandling av personuppgifter i ostrukturerat material. Detta kan tyckas motsägelsefullt eftersom dataskyddsdirektivet som framgått inte medger undantag från artikel 7 vilken alltså motsvaras av 10 § PuL. Av förarbetena till 5 a § framgår emellertid att bedömningen baseras på att den typ av behandling som omfattas av 5 a § kan antas alltid falla in under bestämmelsen 7 f i dataskyddsdirektivet om tillåten behandling efter en intresseavvägning och att det enligt direktivet är tillåtet för medlemsstaterna att närmare precisera hur den angivna intresseavvägningen utfaller i olika fall (prop. 2005/06:173 s. 33 f.).

Som redan nämnts finns utöver uppräkningen i 10 § ytterligare restriktioner som träffar myndigheters behandling av speciella uppgiftskategorier, nämligen känsliga personuppgifter samt personnummer eller samordningsnummer. Dessa restriktioner berörs mer ingående nedan i avsnitt 9.3. Innebär en personuppgiftsbehandling att uppgifter överförs till tredjeland, dvs. till en stat som inte ingår i EU eller EES, måste också 33–35 §§ följas. Myndigheters överföring av personuppgifter till tredjeland behandlas i kapitel 12.

Förslaget till uppgiftsskyddsförordning

Kommissionen

Kommissionens förslag till uppgiftsskyddsförordning motsvarar i grunden de principer och kriterier för under vilka förutsättningar behandling av personuppgifter är tillåten som anges i dataskyddsdirektivet.

Artikel 5 i uppgiftsskyddsförordningen – med rubriken Principer om behandling av personuppgifter – motsvarar artikel 6 i direktivet, dock med några förändringar. Bland annat finns ett tillägg om att uppgifterna ska behandlas på ett öppet sätt i förhållande till den registrerade (öppenhetsprincipen) och ett klargörande beträffande att behandlade uppgifter ska vara begränsade till ett strikt minimum när det gäller de syften för vilka de behandlas; de ska bara behandlas om, och så länge som, syftena inte kan uppnås genom att man behandlar information som inte rör personuppgifter (uppgiftsminimeringsprincipen). Det har vidare uppställts ett krav på att uppgifterna alltid ska vara aktuella, dvs. inte bara när detta är nödvändigt vilket gäller enligt direktivet. Vidare har ordet ”utplånas” i direktivet ersatts med ordet ”raderas” i kommissionens förslag. Dessutom har beträffande den registeransvariges övergripande ansvar tillagts att ansvaret omfattar efterlevnaden av de olika kraven ”vid varje behandling”. Ytterligare vissa justeringar har gjorts.

Genom artikel 21 i förordningen klargörs unionens eller medlemsstaternas befogenheter att behålla eller införa begränsningar av de principer som fastställs i artikel 5. Sådan begränsning får dock bara ske om den är en nödvändig och proportionell åtgärd i ett demokratiskt samhälle och syftar till att garantera vissa uppräknade intressen som i stort överensstämmer med de som omfattas av artikel 13 i dataskyddsdirektivet. En viss skillnad gentemot dataskyddsdirektivet synes dock föreligga genom att det i 21.1 c förordningen hänvisas till ”andra av unionens eller en medlemsstats allmänna intressen, särskilt ett av unionens eller en medlemsstats viktiga ekonomiska eller finansiella intressen, däribland…”. I jämförelse med motsvarande bestämmelse i artikel 13.1 e i direktivet tycks alltså begränsningar för ett allmänt intresse inte bara kunna avse ekonomiska eller finansiella intressen även om det är dessa intressen som i första hand avses komma i fråga. I artikel 21.2 i förordningen föreskrivs att alla begränsningar enligt 21.1 ska innehålla

särskilda bestämmelser åtminstone avseende målen för behandlingen och fastställandet av den personuppgiftsansvarige.

Artikel 6 i kommissionens förslag – med rubriken När personuppgifter får behandlas (Lawfulness of processing) – motsvarar artikel 7 i dataskyddsdirektivet men är utbyggd. Samma rättsliga grunder för behandling, punkterna a–f, återfinns även i uppgiftsskyddsförordningen. En skillnad är att det i artikel 6.1 a i förordningen uttryckligen anges att den enskildes samtycke måste avse behandling för ett eller flera specifika ändamål. Ett samtycke in blanco till personuppgiftsbehandling för ospecifika ändamål är alltså inte en rättsligt godtagbar grund. Detta har dock redan tidigare ansetts gälla – bl.a. genom definitionen av begreppet samtycke i artikel 2 dataskyddsdirektivet om att samtycke ska vara en ”särskild” viljeyttring – och förordningen innebär därvid mest ett klargörande.

När det gäller artiklarna 6.1 c om behandling som är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den registrerade och 6.1 e om behandling som är nödvändig för att utföra en arbetsuppgift av allmänt intresse eller som utförs som ett led i myndighetsutövning som utförs av den registrerade anges i artikel 6.3, att dessa grunder för behandling ska föreskrivas i unionslagstiftningen eller lagstiftningen i den medlemsstat vars lagstiftning den registeransvarige lyder under. Sådan nationell lagstiftning måste uppfylla ett mål av allmänt intresse eller vara nödvändig för att skydda andras fri- och rättigheter, respektera det väsentliga innehållet i rätten till skydd av personuppgifter och vara proportionell mot det legitima mål som eftersträvas.

En nyhet föreskrivs i artikel 6.4 där det anges att när ändamålet med ytterligare behandling inte är förenligt med det ändamål för vilket personuppgifterna har samlats in, måste behandlingen ha en rättslig grund i minst en av de grunder som anges i artikel 6.1 a–e. Detta ska särskilt gälla eventuella ändringar av förutsättningarna och de allmänna villkoren för ett avtal. Bestämmelsen torde innebära en uppmjukning av den s.k. finalitetsprincipen.

Vad gäller artikel 6.1. f om behandling efter en intresseavvägning, dvs. den bestämmelse som motsvarar artikel 7 f i direktivet, föreskrivs att den bestämmelsen inte ska gälla för behandling som utförs av myndigheter i deras myndighetsutövning. I den engelska versionen uttrycks detta med ”…carried out by public authorities in the performance of their tasks.” Den svenska lydelsen, som talar

om myndighetsutövning i stället för en myndighets uppgifter, ger således ett snävare intryck än den engelska. Det kan nämnas att Artikel 29-gruppen har angett att förändringen eventuellt kan komma att leda till en bredare tolkning av vad som är ett allmänt intresse eller myndighetsutövning alternativt att tolkningen av undantaget från intresseavvägningsgrunden kommer att bli restriktiv (Opinion 06/14 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC s 23).

Artikel 7 – med rubriken Villkor för samtycke – har inte någon motsvarighet i dataskyddsdirektivet. Däri föreskrivs bl.a. att den registrerades samtycke inte ska utgöra en rättslig grund för behandlingen, om det föreligger en betydande obalans mellan den registrerades och den registeransvariges ställning (artikel 7.4). Enligt punkt 34 i ingressen till förordningen torde, när den registeransvarige är en myndighet, obalans endast uppkomma vid specifika uppgiftsbehandlingar där myndigheten i kraft av sina offentliga befogenheter kan ålägga skyldigheter och samtycket, med hänsyn tagen till den registrerades intresse, inte kan anses ha lämnats frivilligt.

Europaparlamentet

Europaparlamentet har i sin resolution rörande uppgiftsskyddsförordningen föreslagit vissa ändringar i förordningen.

När det gäller artikel 5 kan nämnas att vad gäller kravet enligt punkten d på att uppgifter ska vara aktuella har parlamentet föreslagit en återgång till att det bara ska gälla om det är nödvändigt. Vidare har parlamentet föreslagit två nya punkter med krav på personuppgiftsbehandlingen, nämligen att de ska behandlas på ett sätt som ger de registrerade möjlighet att effektivt utöva sina rättigheter (effektivitet), och att de ska behandlas på ett sätt som medför ett skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse med hjälp av lämpliga tekniska eller organisatoriska åtgärder (integritet). Parlamentet har vidare föreslagit väsentliga ändringar i artikel 21 om möjligheter att lagstifta om begränsningar, bl.a. har man föreslagit att det inte ska vara möjligt för medlemsstater att genom lagstiftning begränsa skyldigheterna enligt artikel 5.

Beträffande artikel 6.3 har parlamentet föreslagit ett tillägg om att medlemsstaterna inom ramen för bestämmelserna i förordningen får i nationell lagstiftning reglera detaljer som rör behandlingens laglighet, särskilt med avseende på registeransvariga, behandlingsändamål och ändamålsbegränsning, uppgifternas karaktär och de registrerade, behandlingsmetoder och behandlingsförfaranden, mottagare samt lagringstid. Vidare har parlamentet bl.a. förordat en strykning av den av kommissionen föreslagna bestämmelsen i artikel 6.4, som delvis rör finalitetsprincipen.

Parlamentet har vidare föreslagit att bestämmelsen i artikel 7.4 om att samtycke inte är en rättslig grund för behandling, om det föreligger en betydande obalans mellan den registrerades och den registeransvariges ställning, stryks.

Några kommentarer

Vad gäller de allmänna förutsättningarna för myndigheters behandling av personuppgifter kan konstateras att förordningens bestämmelser i grunden bibehåller vad som följer av direktivet. De förändringar som i detta sammanhang kan påtalas särskilt är dels uppmjukningen av finalitetsprincipen, dels att behandling efter en intresseavvägning enligt nuvarande 9 § f PuL inte kommer att vara tillämplig vid myndigheters behandling av personuppgifter, i vart fall inte vid behandling som sker i deras myndighetsutövning.

Vilken betydelse i praktiken det skulle innebära för myndigheter att behandlingar för nya men oförenliga ändamål får ske om den nya behandlingen faller in under någon av de rättsliga grunderna för behandling är svårt att bedöma. Helt klart innebär det – från ett dataskyddsrättsligt perspektiv – ett ökat utrymme för nya behandlingar av redan insamlade personuppgifter. Som vi redan påpekat i olika sammanhang omfattas myndigheternas verksamheter och informationshantering emellertid av annan reglering som sätter gränser för myndigheters aktiviteter, en reglering som delvis leder till samma resultat som den nuvarande finalitetsprincipen varför en sådan förändring troligen skulle få en mindre betydelse för myndigheter än för enskilda personuppgiftsansvariga. Det förefaller för övrigt ganska osäkert om kommissionens förslag i denna del kommer att genomföras.

Även när det gäller den andra förändringen, att behandling efter en intresseavvägning enligt punkten f inte kommer att vara tillämplig vid myndigheters behandling av personuppgifter, anser vi att det inte är troligt att den förändringen får så stor betydelse för myndigheter. De övriga rättsliga grunderna för behandling av personuppgifter oberoende av samtycke täcker, som har framgått, myndigheters behov av personuppgiftsbehandling i deras verksamheter. Något egentligt behov av att kunna behandla personuppgifter efter en intresseavvägning torde alltså inte finnas.

9.2.2 Reglering i registerförfattningar

Registerförfattningar har som redan framgått utformats på olika sätt vad avser bl.a. struktur och begreppsapparat. Det är en tämligen stor skillnad mellan det vi kallar renodlade registerförfattningar, som alltså gäller viss registerföring och som ofta handlar om personuppgiftsbehandling som myndigheter ska utföra, och sådana informationshanteringsförfattningar som reglerar vilken personuppgiftsbehandling som myndigheter får utföra inom vissa närmare angivna verksamheter.

Den förstnämnda kategorin kännetecknas av att författningarna inte lämnar så stort utrymme för den personuppgiftsansvariga myndigheten att göra bedömningar utifrån 9 eller 10 § PuL, i vart fall inte när det gäller myndighetens eget primära handhavande av registret i fråga. Registrets ändamål, vilka personuppgifter som ska samlas in och registreras, hur länge uppgifterna får bevaras m.m., dvs. frågor som annars måste bedömas utifrån de grundläggande kraven i 9 §, är ofta redan reglerade och själva registerföringen är en uppgift för myndigheten som medför sådan nödvändig personuppgiftsbehandling som omfattas av 10 § b (om registret ska föras enligt författningen) eller d eller e (om registret får föras).

Gemensamt för registerförfattningar av den kategori som vi kallar informationshanteringsförfattningar är normalt att det av förarbetsuttalanden eller av direkta hänvisningar till personuppgiftslagen framgår att de grundläggande kraven i 9 § PuL också ska gälla vid behandling av personuppgifter enligt registerförfattningen i fråga medan 10 § ersätts av regleringen i registerförfattningen.

9.2.3 Särskilt om ändamålsbestämning

Den allmänna regleringen

Dataskyddsdirektivet och personuppgiftslagen

Som har framgått följer av artikel 6.1 i dataskyddsdirektivet och 9 § första stycket c och d och andra stycket PuL att personuppgifter ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och att senare behandling av redan insamlade personuppgifter får inte ske för något ändamål som är oförenligt med det eller de ursprungligt angivna ändamålen (finalitetsprincipen).

Det följer av definitionen av begreppet personuppgiftsansvarig i 3 § PuL att det är den personuppgiftsansvarige som har att bestämma och ange de särskilda ändamålen med behandlingen. Det är en skyldighet att se till att ändamålet eller ändamålen är uttryckligt angivna redan när uppgifterna samlas in. Något hinder mot att ange flera parallella insamlingsändamål finns inte alldeles oavsett om de sinsemellan kan tyckas vara oförenliga. Något rättsligt krav på den personuppgiftsansvarige att nedteckna ändamålen eller ändamålet med behandlingen av personuppgifter finns heller inte (prop. 1997/98:44 s. 63 f.). Bestämmelserna i 23–25 §§ PuL om information till den registrerade när personuppgifterna samlas in medför dock som regel att ändamålen måste uppges redan när behandlingen påbörjas. Den personuppgiftsansvarige är därutöver skyldig att uppge ändamålen antingen i anmälan till tillsynsmyndigheten (36 §) eller till var och en som begär en sådan upplysning (42 §) eller i s.k. registerutdrag till den registrerade (26 §).

Enligt personuppgiftslagen krävs vidare att de ursprungliga ändamålen är ”särskilda”. En alltför allmänt eller vagt hållen ändamålsbeskrivning är alltså inte godtagbar. Hur pass detaljerad ändamålsangivelsen ska vara för att uppfylla lagens krav på att vara särskild kunde enligt Datalagskommittén avgöras i praxis eller genom preciserande reglering i förordning eller genom Datainspektionens föreskrifter (SOU 1997:39 s. 350).

Ändamålen ska vidare vara berättigade (”legitimate” i direktivets engelska version). I förarbetena till personuppgiftslagen angavs att det rekvisitet infördes närmast för säkerhets och fullständighets skull eftersom det angavs som ett krav i artikel 6 i dataskyddsdirektivet. Det är dock, på samma sätt som nämnts ovan beträff-

ande kravet på lagenlighet enligt 9 § första stycket a PuL, osäkert om bestämmelsen om berättigade ändamål har någon självständig betydelse. I vilka fall det är berättigat att samla in och behandla personuppgifter följer ju indirekt av personuppgiftslagen.

Finalitetsprincipen – senare behandling av insamlade personuppgifter för nya ändamål

Om en tilltänkt behandling av redan insamlade personuppgifter inte direkt omfattas av de ursprungliga ändamålen måste det prövas om ändamålet med den senare behandlingen är oförenligt med de ursprungliga ändamålen. Detta följer av 9 § första stycket d. Det är genom den bestämmelsen finalitetsprincipen kommer till uttryck. Datalagskommittén (SOU 1997:39) uttalade att vad som är oförenligt med de ursprungliga ändamålen får bestämmas genom praxis och de mer preciserade regler som regeringen och Datainspektionen kan utfärda (a. bet. s. 351).

Bestämmelsen i 9 § första stycket d PuL medför bl.a. att det är väsentligt att alla de ändamål för vilka man kan tänkas behöva använda insamlade uppgifter finns angivna redan då uppgifterna samlas in. Enligt Registerförfattningsutredningen (SOU 1999:105 s. 253) antydde begreppet ”oförenligt” som sådant att det finns visst utrymme för tolkningen att behandling som sker efter insamlandet inte direkt måste motsvaras av ett från början givet ändamål utan ett visst spelrum torde alltså finnas. Socialdatautredningen resonerade kring oförenlighetsrekvisitet, i ett ofta åberopat uttalande, genom att anföra att man vid en ”oförenlighetsprövning” bör hypotetiskt utgå från hur en registrerad typiskt sett, alltså inte den registrerade i det enskilda fallet, skulle se på saken. Kommer man vid en sådan bedömning fram till att den registrerade rimligen har att räkna med att de insamlade personuppgifterna också får behandlas för det nya ändamålet, kan det nya ändamålet inte anses vara oförenligt med det ursprungliga ändamålet (SOU 1999:109 s. 160).

Finalitetsprincipen aktualiseras bl.a. då en personuppgiftsansvarig lämnar ut uppgifter till en annan personuppgiftsansvarig för att användas av denne för något eget ändamål. Mottagarens ändamål får då inte vara oförenligt med utlämnarens ursprungliga ändamål. Om så är fallet strider utlämnarens behandling mot finalitetsprin-

cipen. Mottagarens behandling, å andra sidan, torde i så fall kunna strida mot 9 § första stycket a och b PuL om att behandlingen ska vara laglig och korrekt.

I doktrinen har det hävdats att en registrerad inte med rättslig verkan kan samtycka till att personuppgifter behandlas i strid med finalitetsprincipen. Om den registrerade ger sitt samtycke till att redan insamlade personuppgifter används för nya ändamål som är oförenliga med de som var bestämda vid insamlandet, får detta anses jämställt med en ny insamling av personuppgifterna. Det är alltså inte nödvändigt att samla in personuppgifterna en gång till (Öman/Lindblom, s. 204). Artikel 29-gruppen har dock anlagt ett annat synsätt som innebär att inhämtande av särskilt samtycke till behandling för ett nytt ändamål är en omständighet, ett slags kompensatorisk faktor, bland flera omständigheter som kan tillmätas relevans när det ska bedömas om den nya behandlingen är oförenlig med det ursprungliga ändamålet eller inte (Data Protection Working Party, Opinion 03/2013 on purpose limitation, 00569/13/EN WP 203, s. 27).

Ändamålsbestämning i registerförfattningar

Allmänt

Utgångspunkten är alltså att det följer av personuppgiftslagen att det är den personuppgiftsansvarige som bestämmer för vilka ändamål personuppgifter behandlas. I registerförfattningar anges emellertid regelmässigt uttryckligen i författningen de ändamål för vilka personuppgifter får behandlas. Regeringen har, bl.a. i motiven till studiestödsdatalagen (2009:287), uttryckt att det i en speciallag som riktar sig mot en särskilt angiven verksamhet faller sig naturligt att direkt i lagen ange för vilka ändamål personuppgifter får behandlas på det mer avgränsade område lagen avser att täcka (prop. 2008/09:96 s. 40.).

Syftet med ändamålsbestämmelser i registerförfattningar är normalt att ange en yttersta ram inom vilken uppgifterna får behandlas (se t.ex. prop. 1997/98:97 s. 121, prop. 2000/01:33 s. 99 och SOU 2006:82 s. 178). Ramen gäller alla typer av behandlingar som kan komma ifråga (jfr definitionen av behandling av personuppgifter i 3 § PuL). Ändamålsbestämmelser är därför av central betydelse i dessa för-

fattningar. I många registerförfattningar förekommer ändamålsbestämmelserna under rubriker som ”Ändamål”, ”Ändamålen med behandlingen” eller ”När behandling av personuppgifter är tillåten”.

Preciseringen av ändamål

Ändamålen ska alltså enligt 9 § första stycket c PuL vara särskilda, dvs. ändamålsangivelserna får inte vara alltför allmänt hållna. Det ligger dock i sakens natur att när ändamål regleras genom författningsbestämmelser dessa ofta måste formuleras ganska generellt, det gäller särskilt beträffande det vi kallar informationshanteringsförfattningar.

När det gäller frågan om vilken grad av precisering som kan krävas har Socialdatautredningen påpekat att viss ledning kan fås av bestämmelserna i 9 § första stycket e och f PuL om att det är ett grundläggande krav att personuppgifter som behandlas ska vara adekvata och relevanta i förhållande till ändamålen med behandlingen samt att inte fler personuppgifter får behandlas än som är nödvändigt med hänsyn till ändamålen. Om inte ändamålet eller ändamålen har en viss grad av precision, kan man knappast bedöma huruvida personuppgifterna är adekvata och relevanta eller för många (SOU 1999:109 s. 156). I motiven till lagen (2001:454) om behandling av personuppgifter inom socialtjänsten anfördes att ändamålen bör vara så preciserade att förhållandena utgör ett tillräckligt skydd för den personliga integriteten samtidigt som de inte utgör ett hinder vid förändring av verksamheten (prop. 2000/01:80 s. 142). I det lagstiftningsärendet frångick regeringen Socialdatautredningens förslag om att de närmare ändamålen skulle bestämmas av personuppgiftsansvarig myndighet. I lagen anges under rubriken När behandling av personuppgifter är tillåten att personuppgifter får behandlas bara om behandlingen är nödvändig för att arbetsuppgifter inom socialtjänsten ska kunna utföras. Lagrådet anmärkte att en sådan bestämmelse framstår som en motsvarighet till 10 § PuL och inte som en ändamålsbestämning, något som Lagrådet ansåg var en brist (a. prop. s. 272). Regeringen fann dock att det var lämpligare att reglera ändamålen i förordning. Den aktuella bestämmelsen kompletteras därför med att regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om begränsning av

tillåtna ändamål. Regeringen har i förordningen (2001:637) om behandling av personuppgifter inom socialtjänsten meddelat närmare föreskrifter om tillåtna ändamål.

Ändamålsregleringen på socialtjänstens område är dock inte typisk. I de fall det är fråga om en registerlag som kompletteras av bestämmelser i en anslutande förordning är de närmare ändamålsbestämmelserna oftast intagna på lagnivå och inte i förordning. Skälet till detta torde vara att, mot bakgrund av ändamålsbestämningens centrala roll för persondataskyddet, det sedan länge har ansetts som principiellt viktigt att riksdagen beslutar ändamål för stora och integritetskänsliga personregister. Samma synsätt har präglat utformningen av senare decenniers författningar som reglerar personuppgiftsbehandling vid informationshantering i viss verksamhet och inte bara vid förandet av ett visst register. I en hel del informationshanteringsförfattningar anges i förarbetena att ändamålsbestämmelserna är den yttre ramen för den tillåtna personuppgiftsbehandlingen inom tillämpningsområdet samt att det förutsätts eller krävs att den personuppgiftsansvariga myndigheten anger mer preciserade ändamål för specifika behandlingar inom den tillåtna ramen. I registerförfattningar förekommer vidare föreskrifter om att regeringen eller den myndighet som regeringen bestämmer får föreskriva begränsningar i förhållande till lagens ändamålsbestämmelser. Ett exempel är 6 § lagen (2002:546) om behandling av personuppgifter i den arbetsmarknadspolitiska verksamheten.

Vad gäller innehållet i de specifika ändamål som anges i de olika informationshanteringsförfattningarna skiljer de sig åt beroende på vilken verksamhet som avses. I motiven har normalt gjorts vissa generella uttalanden angående vad som behöver anges i ändamålsbestämmelserna.

I lagstiftningsärendet angående lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet uttalade Lagrådet att en särskild ändamålsbestämmelse som ger stöd för att uppgifter som behandlas i verksamheten även får behandlas för planering, uppföljning och utvärdering är obehövlig (prop. 2004/05:164 s. 179). Lagrådet ansåg att planering, uppföljning och utvärdering av verksamhet är en integrerad del av själva verksamheten och inte någon fristående aktivitet som behöver regleras särskilt. Behandling av personuppgifter för dessa ändamål får alltså ske utan att det uttryckligen framgår av de i lagen angivna ändamålen. Liknande

bedömningar har även gjorts i senare lagstiftningsärenden (se t.ex. prop. 2009/10:85: s. 116).

Det förekommer dock att planering, uppföljning och utvärdering anges som särskilda uttryckliga ändamål i registerförfattningar, t.ex. i 114 kap. 7 § 5 socialförsäkringsbalken, 3 § andra stycket lagen (2001:617) om behandling av personuppgifter inom kriminalvården och 2 kap. 4 § 5 patientdatalagen (2008:355). I motiven till patientdatalagen anfördes att behovet av att särskilt ange för vilka ändamål personuppgifter ska få behandlas måste bedömas från fall till fall, med utgångspunkt från bl.a. hur övriga ändamålsbestämmelser är utformade i den aktuella författningen (prop. 2007/08:126 s. 58 f.). En tydlig ändamålsreglering kräver att ändamålen formuleras specifikt och med en hög konkretiseringsgrad och till följd härav bör planering, uppföljning och utvärdering, enligt motiven, uttryckligen anges i lagens uppräkning av ändamål. Det kan här nämnas att Patientdatautredningen beträffande ändamålen verksamhetsuppföljning och kvalitetssäkring anförde att de behövde anges som självständiga ändamål eftersom det i vissa fall kunde förekomma insamling av personuppgifter för dessa ändamål., t.ex. i form av brukarenkäter eller kvalitetsregisterföring, och inte bara sekundär återanvändning för dessa syften av redan insamlade personuppgifter för det primära ändamålet vårddokumentation (SOU 2006:82 s. 185 f.).

En registerförfattning kan vidare innehålla dels generella ändamålsbestämmelser avseende all personuppgiftsbehandling inom en viss verksamhet, dels ändamålsbestämmelser som endast avser ett visst register eller databas som regleras i registerförfattningen. Ett exempel är lagen (2001:184) om behandling av personuppgifter i Kronofogdemyndighetens verksamhet. I lagen särregleras personuppgiftsbehandlingen i fyra olika databaser, där varje databas har egna ändamålsbestämmelser.

Behandling som är nödvändig eller som behövs

I personuppgiftslagen används dataskyddsdirektivets nödvändighetsbegrepp när det t.ex. handlar om att inte fler personuppgifter får behandlas än vad som är nödvändigt med hänsyn till ändamålen liksom beträffande i vilka situationer behandling kan vara tillåten

utan den registrerades samtycke (artikel 6 d och 7 b–f direktivet och 9 § f och 10 § a–f PuL). I många informationshanteringsförfattningar används nödvändighetsbegreppet även i ändamålsbestämmelser. Det förekommer emellertid också att det i stället anges att personuppgifter får behandlas om det behövs för ett visst ändamål osv. Så är t.ex. fallet beträffande informationshanteringsförfattningarna för Skatteverkets beskattningsverksamhet och folkbokföring, Tullverkets tullverksamhet, Kronofogdemyndigheten, Arbetsförmedlingens arbetsmarknadspolitiska verksamhet, hälso- och sjukvården (patientdatalagen) samt Centrala studiestödsnämnden (studiestödsdatalagen). Såvitt kan utläsas av förarbetena finns inga indikationer på att uttryckssättet ”behövs” betydelsemässigt skulle åsyfta något annat än vad som avses med nödvändighetsbegreppet i personuppgiftslagen. I vart fall framgår ingen sådan avsedd skillnad av motiven. I motiven till studiestödsdatalagen har i stället klargjorts att med att ”behandlingen behövs” för olika syften avses detsamma som när det i 10 § PuL anges att behandlingen är nödvändig (prop. 2008/09:96 s. 134).

Primära och sekundära ändamål

Det förekommer vidare att det i registerförfattningar görs en uppdelning av ändamålen i primära och sekundära sådana. De primära ändamålen avses tillgodose den behandling som behövs i myndighetens egna verksamhet medan de sekundära ändamålen tar sikte på myndighetens utlämnande av uppgifter för att tillgodose andras behov. Syftet är således att göra det tydligt hur uppgifterna får användas i den egna verksamheten och i vilka syften de får lämnas ut till andra. Ett utlämnande av personuppgifter som sker som ett led i den egna verksamheten, inte i syfte att tillgodose andras behov, anses vanligtvis omfattas av de primära ändamålen (Sören Öman, Särskilda registerförfattningar, Festskrift till Peter Seipel, s. 699 f.).

De primära ändamålen kan alltså sägas vara styrande för vilka personuppgifter som får samlas in hos myndigheten. I doktrinen har hävdats att relationen mellan de primära och sekundära ändamålen får förstås så att behandling för att lämna ut personuppgifter till annan enligt de sekundära ändamålen bara får avse person-

uppgifter som myndigheten samlat in och i övrigt behandlat för sina egna primära ändamål. Att ett utlämnande enligt de sekundära ändamålen endast avser sådana personuppgifter som får behandlas enligt de primära ändamålen framgår ibland av författningstexten i registerförfattningarna. Regleringen i 2 kap. 7 och 8 §§ polisdatalagen är ett exempel på detta, dvs. att det framgår att behandling för sekundära ändamål bara får avse personuppgifter som redan samlats in för primära ändamål. Detta framgår av att det i 8 §, som reglerar de sekundära ändamålen, uttryckligen anges att personuppgifter som redan behandlas enligt 7 §, dvs. för primära ändamål, även får behandlas när det är nödvändigt för att tillhandahålla information som behövs i annan verksamhet.

Regleringen i 1 kap. 4 och 5 §§ lagen (2001:181) om behandling av uppgifter i Skatteverkets beskattningsverksamhet har en annan konstruktion. Där anges det inte att de sekundära ändamålen som listas i 5 § endast avser behandling av uppgifter som redan har samlats in och behandlas av Skatteverket för något av de primära ändamål som anges i 4 §. Enligt denna lagtekniska utformning finns det således inget som i och för sig hindrar att Skatteverket samlar in personuppgifter för ändamål som bara tillgodoser andra aktörers behov så länge som dessa behov återfinns bland de sekundära ändamålen i lagens 1 kap. 5 §. Syftet med regleringen tycks emellertid ha varit att de sekundära behoven i allt väsentligt ska avse uppgifter som Skatteverket redan har samlat in för den egna verksamhetens behov, dvs. att de sekundära ändamålen avser ett slags återanvändning. På så sätt liknar regleringen den i polisdatalagen, även om detta alltså inte har kommit till uttryck i utformningen av regleringen.

Ytterligare en skillnad i utformningen av ändamålsregleringen i registerförfattningarna är att det dels förekommer uttömmande bestämningar av samtliga ändamål – såväl primära som sekundära – för vilka behandling får ske, dels den varianten att de i författningen angivna ändamålen kompletteras med en möjlighet att vidarebehandla redan insamlade uppgifter även för ändamål som inte är oförenliga med insamlingsändamålet. Skillnaden består således i att lagstiftaren i det senare fallet har gett den personuppgiftsansvariga myndigheten utrymme att själv bestämma kompletterande ”sekundära” ändamål. Det är alltså myndigheten själv som måste beakta finalitetsprincipen. Man brukar då tala om att ”finalitetsprincipen

tillämpas” men vad som i strikt rättslig mening avses är snarare en tillämpning av bestämmelsen i 9 § första stycket d PuL.

Ändamålsbestämmelser och uppgiftsutlämnande

Särskilt beträffande myndigheters personuppgiftsbehandling genom utlämnande av personuppgifter har finalitetsprincipen varit föremål för diskussion eftersom det inte sällan uppstått osäkerhet kring frågan om förhållandet mellan denna princip, ändamålsbestämmelser i registerförfattningar och bestämmelser i bl.a. offentlighets- och sekretesslagen som föreskriver utlämnande eller medger att uppgifter lämnas ut utan hinder av sekretess. Enligt t.ex. 6 kap. 5 § OSL ska en myndighet på begäran av en annan myndighet lämna uppgift som den förfogar över, om inte uppgiften är sekretessbelagd eller det skulle hindra arbetets behöriga gång. Skyldigheten anses utgöra en precisering av den allmänna samverkansskyldighet som gäller för myndigheter enligt 6 § FL. Det har ifrågasatts om denna skyldighet står i strid med finalitetsprincipen och därmed dataskyddsdirektivet.

Offentlighets- och sekretesskommittén uttalade i sitt huvudbetänkande Ny sekretesslag (SOU 2003:99 s. 231 f.) att regering och riksdag redan vid personuppgiftslagens tillkomst fick anses ha tagit ställning till att bestämmelsen i 15 kap. 5 § SekrL (numera 6 kap. 5 § OSL) inte strider mot dataskyddsdirektivet. Det beror på att den detaljerade sekretessregleringen avseende integritetskänsliga uppgifter gäller även i förhållandet mellan myndigheter och mellan självständiga verksamhetsgrenar inom samma myndighet, dock att lagstiftaren har infört sekretessbrytande regler som innebär att sekretesskyddade uppgifter under vissa förutsättningar kan lämnas ut till annan myndighet. Kommittén fortsatte (a. bet. s. 232):

> Genom denna ordning uppnås samma syfte som man vill åstadkomma genom finalitetsprincipen. Myndigheterna hindras att lämna ut integritetskänsliga uppgifter till andra myndigheter, för ändamål som av lagstiftaren bedömts vara oförenliga med de ändamål för vilka uppgifterna samlats in. De uppgifter som inte försetts med något sekretesskydd eller som omfattas av sekretessbrytande regler har av lagstiftaren ansetts vara av sådan karaktär att utlämnanden till andra myndigheter, eller, när det gäller sekretessbrytande regler, vissa myndigheter, inte kan anses vara oförenliga med det ändamål för vilket

> uppgifterna samlats in. Detta ställningstagande kommer till uttryck i [dåvarande] 15 kap. 5 § sekretesslagen.

Offentlighets- och sekretesskommittén resonerade på samma sätt rörande utlämnande av sekretesskyddade uppgifter som sker på en myndighets eget initiativ, eftersom utlämnandet även i sådant fall måste ske med stöd av en sekretessbrytande bestämmelse. När de sekretessbrytande bestämmelserna införts har lagstiftaren, anförde kommittén, gjort en avvägning mellan intresset av att uppgiften lämnas ut och intresset av att skydda enskilda personers integritet. För enskilda måste det anses stå klart att utlämnande med stöd av sekretessbrytande bestämmelser kan komma att ske.

Kommitténs bedömningar är emellertid inte okontroversiella. Det har hävdats att kommitténs tolkning av finalitetsprincipen i detta avseende är synnerligen liberal (Öman/Lindblom, s. 167).

Såvitt avser finalitetsprincipens tillämplighet på registerförfattningarnas område anförde kommittén vidare följande (SOU 2003:99 s. 236 f.).

> När det gäller frågan om ett utlämnande mellan myndigheter enligt sekretesslagen är förenligt med finalitetsprincipen som den kommer till uttryck i registerförfattningarna bör samma bedömning som ovan redovisats göras. Ett uppgiftslämnande till en annan myndighet skall anses förenligt med finalitetsprincipen om det är tillåtet enligt sekretesslagen, annars inte.
>
> Beträffande utlämnanden som sker på begäran av en annan myndighet och där alltså 15 kap. 5 § sekretesslagen är tillämplig kan det dessutom hävdas att utlämnandet skall ske på grund av lex specialis. En särskild lag om behandling av personuppgifter anger vanligtvis generellt i vilka fall behandling av en uppgift får ske. Ett utlämnande av uppgiften är en av många olika slags behandlingar av uppgiften. En bestämmelse om uppgiftsskyldighet avser emellertid en specifik behandling. Bestämmelserna om uppgiftsskyldighet bör därmed betraktas som lex specialis i förhållande till en mer generell bestämmelse om när uppgifter får behandlas och gälla i första hand.
>
> […]
>
> Om det visar sig vara så att en särskild lag om behandling av personuppgifter uttömmande anger i vilka fall uppgifter får lämnas är finalitetsprincipen inte tillämplig. Skulle utlämnandet ske efter begäran bör det närmast vara 15 kap. 5 § sekretesslagen som utgör den generella lagstiftningen, medan den särskilda lagen om behandling av personuppgifter blir lex specialis i förhållande till 15 kap. 5 §. Bestäm-

melserna i registerlagstiftningen skulle alltså i detta fall gå före sekretesslagen och utlämnandet utgöra en otillåten behandling.

Även Integritetsskyddskommittén har berört frågeställningen om ändamålsbestämmelser i registerförfattningar och finalitetsprincipen samt påpekat att oklarheterna härvidlag och bristen på samordning och enhetlighet i utformningen av registerförfattningarna medför svårigheter i tillämpningen och överblickbarheten i regelverket, vilket i sin tur innebär en risk för onödiga integritetsintrång, se delbetänkandet Skyddet för den personliga integriteten – Kartläggning och analys (SOU 2007:22 s. 462).

Såvitt avser registerförfattningars ändamålsbestämmelser anförde kommittén bl.a. följande (a. bet. s. 465 f.).

> Bestämmelser om sekundära ändamål är emellertid problematiska från den synpunkten att de ibland också avses ge svar på frågan om när uppgifter får lämnas ut. Ibland avser de sekundära ändamålen att uttömmande reglera för vilka ändamål och till vilka som uppgifter får lämnas ut. Så är fallet i den reglering som avser behandling av personuppgifter inom Tullverkets brottsbekämpande verksamhet. Där synes bestämmelserna syfta till att, i betydligt större omfattning än vad som gäller enligt sekretesslagen, inskränka möjligheterna att lämna ut uppgifter till andra myndigheter. Om bestämmelserna skall tillämpas i enlighet med detta syfte torde man för uppgifter som behandlas i enlighet med lagen – vilket bör vara i stort sett alla uppgifter eftersom handläggningen i allt väsentligt är datoriserad – i praktiken ha infört en absolut sekretess i förhållande till andra myndigheter, trots att det i sekretesslagen anges att sekretess på detta område gäller med ett omvänt skaderekvisit.
>
> Bestämmelser om sekundära ändamål kan också vara avsedda att inte uttömmande ange när uppgifter får lämnas ut. Ett sådant syfte framgår i allmänhet inte av lagtexten, men brukar anges i förarbetena. På skatteområdet omfattar de sekundära ändamålen utlämnande till såväl myndigheter som till enskilda som bedriver författningsreglerad verksamhet. I lagtexten görs ingen skillnad mellan utlämnanden som sker på grund av uppgiftsskyldighet, efter en sekretessprövning enligt 14 kap. 3 § sekretesslagen eller därför att det är fråga om utlämnande av offentliga uppgifter. Bestämmelsen synes snarast utgöra någon slags exemplifiering av när utlämnanden kan komma att ske (jfr prop. 2000/01:33 s. 99). Även denna typ av bestämmelser försvårar möjligheterna att avgöra vilket skydd respektive vilka inskränkningar i den enskildes integritet som det är fråga om.

> Ett grundläggande problem i sammanhanget synes vara att inte heller när det gäller bestämmelser i registerförfattningar om ändamål med behandlingen har lagstiftaren på något enhetligt sätt tagit ställning till hur sådana regler förhåller sig till bestämmelser i andra lagar som också kan ha betydelse i sammanhanget. Problemet behandlades bland annat av Lagrådet beträffande förslaget om lagstiftning för behandling av personuppgifter på socialförsäkringsområdet (prop. 2002/03:135 s. 159 f.).

I våra direktiv anför regeringen att såsom Integritetsskyddskommittén uppmärksammat förekommer det numera sådana uttömmande ändamålsregleringar som leder till att ett utlämnande av uppgifter mellan myndigheter som är tillåtet enligt offentlighets- och sekretesslagen är förbjudet enligt registerförfattningen. Enligt regeringens mening bör utgångspunkten vara att ändamålsregleringar som utesluter en tillämpning av finalitetsprincien inte ska förekomma. För att undvika oklarheter beträffande huruvida finalitetsprincipen får tillämpas, dvs. att myndigheten kan göra en egen bedömning av om nya ändamål är oförenliga med ursprungliga ändamål eller inte – för att exempelvis bedöma om en vidarebehandling av personuppgifter som inte uttryckligen anges i de reglerade ändamålen är tillåten eller inte – finns det i nyare registerförfattningar inte sällan uttryckliga hänvisningar till regeln i 9 § första stycket d PuL alternativt att en bestämmelse med motsvarande innehåll tagits in i författningen. Ett exempel är 2 kap. 5 § patientdatalagen där det framgår att personuppgifter som samlats in och behandlas för primära ändamål enligt 2 kap. 4 § också får behandlas för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning samt att i övrigt gäller 9 § första stycket d och andra stycket PuL. Ändamålsregleringen i patientdatalagen är emellertid uttömmande i den meningen att vårdgivare inte själva får besluta om ytterligare primära ändamål för vilket eller vilka personuppgifter kan samlas in i och behandlas i verksamheten, i vart fall inte utan den registrerades uttryckliga samtycke.

Men det finns också från senare tid exempel på författningar som innehåller en uttömmande ändamålsbeskrivning även såvitt avser användning av insamlade uppgifter för nya ändamål. Exempelvis har lagen (2013:794) om vissa register för forskning om vad arv och miljö betyder för människors hälsa utformats på så sätt att det inte lämnats något utrymme åt den personuppgiftsansvariga

myndigheten att göra en egen bedömning av om nya ändamål är oförenliga med ursprungliga ändamål eller inte.

I förarbetena till sådana bestämmelser har det brukat anges att personuppgiftslagens finalitetsprincip därmed inte är tillämplig (se t.ex. prop. 2012/13:163 s. 50). Det kan emellertid hävdas att innebörden av uttömmande ändamålsregleringar av det slaget också kan beskrivas på det sättet att lagstiftaren redan har tillämpat finalitetsprincipen och därvid funnit att varje nytt ändamål skulle vara oförenligt med de författningsreglerade ändamålen. Registerförfattningens ändamålsreglering är alltså snarare ett uttryck för finalitetsprincipen så som den tillämpats av lagstiftaren.

Avslutningsvis finns det skäl att erinra om att även om en ändamålsreglering är uttömmande så är, utan att detta särskilt anges, en behandling av personuppgifter som sker för att uppfylla offentlighetsprincipen enligt 2 kap. TF under alla förhållanden alltid tillåten. Detta följer av grundlags företräde framför vanlig lag.

9.2.4 Våra överväganden och förslag

Personuppgiftslagens grundläggande krav ska gälla även då myndigheter behandlar personuppgifter

Förslag: De grundläggande kraven på behandling av personuppgifter i 9 § PuL ska tillämpas då myndigheter behandlar personuppgifter. Detta ska gälla oberoende av om behandlingen sker i s.k. strukturerat eller ostrukturerat material. I den nya lagen ska detta tydliggöras genom en hänvisning till 9 § PuL.

Principerna om uppgifternas kvalitet i dataskyddsdirektivets artikel 6 – eller de grundläggande kraven på behandling av personuppgifter som principerna benämns i 9 § PuL – är några av de mest centrala och grundläggande i den dataskyddsrättsliga regleringen.

Att myndigheter ska uppfylla de grundläggande dataskyddsrättsliga principerna vid behandling av personuppgifter får anses självklart och någon annan generell ordning torde strida mot dataskyddsdirektivets krav.

Däremot skulle det måhända kunna hävdas att de grundläggande kraven i 9 § PuL i hög grad ändå redan gäller indirekt för myn-

digheterna genom annan reglering. Exempelvis ställer objektivitetsprincipen och likhetsprincipen enligt 1 kap. 9 § RF, allmänna förvaltningsrättsliga principer såsom dessa kommer till uttryck i förvaltningslagen, reglerna om handlingsoffentlighet och insyn enligt 2 kap. TF, offentlighets- och sekretesslagens och arkivlagens regler om ordning och bevarande av allmänna handlingar m.m. samt myndighetsinstruktioner och andra regleringar som styr vilka uppgifter en myndighet har, sammantaget krav på myndigheterna att bara behandla personuppgifter lagligt och korrekt, att samla in uppgifter bara för författningsreglerade syften eller annars bestämda och berättigade ändamål, att se till att personuppgifter är riktiga och att korrigera felaktigheter osv.

Vid dataskyddsdirektivets implementering i Sverige fördes det inte något resonemang om huruvida det redan fanns nationell reglering som motsvarade kraven i artikel 6.1 när det gäller personuppgiftsbehandling i myndigheters informationshantering och vilken betydelse detta i så fall skulle ha.

Som vi ser det är det med tanke på kopplingen mellan de grundläggande kraven i 9 § PuL och dels den registrerades rättigheter, t.ex. att kunna göra anspråk på skadestånd för kränkning vid behandling i strid mot bl.a. 9 § PuL, dels tillsynsmyndighetens befogenheter, emellertid uppenbart att den särskilda regleringen i 9 § har en självständig betydelse även på myndighetsområdet. Detta alldeles oavsett att motsvarande krav på personuppgiftsbehandlingen i vart fall delvis kan härledas ur annan reglering som har betydelse för myndigheternas informationshantering. Den dataskyddsrättsliga regleringen med specifika skyldigheter, rättigheter och ett eget sanktionssystem utgör nämligen en rättslig dimension som går utöver den som följer av annan reglering av myndigheters informationshantering. Vidare är det av praktiska skäl givetvis en fördel om regleringen är heltäckande och tydlig i fråga om vilka skyldigheter som myndigheten har vad gäller just personuppgiftsbehandling.

Till detta kommer alltså att det under alla förhållanden knappast torde vara förenligt med dataskyddsdirektivet att enbart förlita sig på att annan redan befintlig reglering av myndigheternas informationshantering skulle vara tillräcklig för att fullt ut garantera det skydd som artikel 6 föreskriver. De grundläggande kraven i 9 § PuL bör således gälla även enligt den generella lag som vi föreslår. Vi ser

ingen anledning att reglera detta på något annat sätt än genom en hänvisning till den paragrafen. Nästa fråga blir då om hänvisningen till 9 § ska gälla utan undantag. Vi återkommer till den frågan i det följande.

Vi har i avsnitt 8.3.2 gjort bedömningen att den s.k. missbruksregeln i 5 a § PuL inte bör vara tillämplig vid myndigheters behandling av personuppgifter. Därmed följer att de grundläggande kraven enligt 9 § måste följas av myndigheter även vid behandling av personuppgifter i ostrukturerat material, t.ex. vid e-posthantering, på webbplatser eller i sociala medier m.m. Som har framgått ser vi det som en självklarhet att myndigheter i sin informationshantering alltid ska följa sådana basala krav på laglighet, korrekthet, ändamålsbestämning, adekvans, riktighet och återhållsamhet m.m. som 9 § PuL ger uttryck för. Vi har inte heller kunnat identifiera något reellt eller berättigat behov för myndigheterna till avvikelser från något av paragrafens grundläggande krav. Till detta kommer att det av annan reglering alltså följer att myndigheterna ska hantera personuppgifter på ett sätt som står i samklang med 9 § PuL och detta gäller givetvis alldeles oavsett om behandlingen sker i strukturerad eller ostrukturerad form. Någon bestämmelse som i något avseende kompenserar för att missbruksregeln inte ska vara tillämplig i fråga om de grundläggande kraven vid behandling av personuppgifter i ostrukturerat material anser vi alltså inte vara motiverad.

Ändamålsbestämning

Bedömning: Någon begränsning av för vilka ändamål myndigheter får behandla personuppgifter bör inte införas i den nya lagen. Därmed blir huvudregeln att det är den personuppgiftsansvariga myndigheten som, inom ramen för sitt uppdrag, har att närmare specificera för vilket eller vilka ändamål personuppgifter behandlas i verksamheten. Dessa ändamål måste uppfylla det grundläggande kravet på att vara särskilda och uttryckligt angivna redan vid insamlingen.

Det kan dock på vissa områden, t.ex. i fråga om särskilt integritetskänsliga informationssamlingar, finnas anledning att genom särskilda föreskrifter i lag eller förordning om ända-

målsbegränsningar ange ramar för myndigheters personuppgiftsbehandling. Sådana föreskrifter kan tas in i bilaga till lagen eller i annan lag eller förordning.

En grundläggande princip i dataskyddsregleringen är alltså att den personuppgiftsansvarige, senast när personuppgifter samlas in, ska ange särskilda ändamål för den planerade behandlingen. Dessa ändamål sätter gränser för hur uppgifterna därefter får behandlas. Både dataskyddsdirektivet och den föreslagna uppgiftsskyddsförordningen öppnar dock för att medlemsstaterna i sin lagstiftning kan bestämma ändamålen för behandlingen (se dataskyddsdirektivets definition av personuppgiftsansvarig i artikel 2, motsvarande bestämmelse finns i artikel 4 i uppgiftsskyddsförordningen).

Vid vår inventering och genomgång av befintliga registerförfattningar, i synnerhet beträffande sådana som vi kallar informationshanteringsförfattningar, har vi kunnat konstatera att många ändamålsbestämmelser inte tycks leva upp till de krav som ställs på att bestämda ändamål ska vara särskilda och bestämda (9 § första stycket c PuL). Ofta är tillämpningsområdet för en informationshanteringsförfattning beskrivet som ett visst slags verksamhet hos en personuppgiftsansvarig myndighet. Ibland är de primära ändamålen i lagens ändamålsbestämmelser i princip identiska med det beskrivna tillämpningsområdet. Ett exempel är polisdatalagen som har tillämpningsområdet den brottsbekämpande verksamheten. Denna består av verksamhet för att förebygga, förhindra eller upptäcka brottslig verksamhet samt utreda och beivra brott. Samma kriterier utgör tillåtna primära ändamål enligt lagen vid sidan om ändamålet diarieföring (1 kap. 2 § samt 2 kap. 7 och 9 §§ polisdatalagen). Den föreslagna domstolsdatalagen har en liknande konstruktion med ett tillämpningsområde, rättskipande och rättsvårdande verksamhet, som i realiteten är identiskt med det tillåtna primära ändamålet enligt lagen, handläggning av mål och ärenden (Ds 2013:10).

Det är tydligt att på så sätt angivna ändamålsbeskrivningar knappast har som syfte att utgöra egentliga ändamålsbestämningar. Syftet är snarare att ändamålsbeskrivningen ska utgöra en precisering i förhållande till 10 § PuL av när personuppgifter alls får behandlas i en viss verksamhet och ofta även i förhållande till 15–20 §§ PuL såvitt avser känsliga personuppgifter. Ett ofta uttalat

syfte är att på så sätt sätta en ram för personuppgiftsbehandlingen inom vilken den personuppgiftsansvarige måste bestämma sådana särskilda, uttryckliga och berättigade ändamål som avses i 9 § första stycket c PuL (se t.ex. prop. 2007/08:126 s. 227 f.). Man kan alltså säga att det har kommit att ske en sammanblandning mellan vad som i dataskyddsrättslig mening är särskilda bestämda ändamål respektive tillåtna rättsliga grunder för behandling. Detta kan tyckas vara otillfredsställande från rent systematisk utgångspunkt. Det finns vidare från integritetsskyddssynpunkt, menar vi, vissa problem med sådana vida ändamålsbestämningar som nyss nämnts. Det finns nämligen en risk för att tillämparen sammanblandar ändamål med rättslig grund och godtar ett i författning bestämt allmänt ändamål som ett i och för sig särskilt och tillräckligt preciserat ändamål och därför drar den felaktiga slutsatsen att personuppgiftslagens krav är uppfyllda. Ett belysande exempel är uppgiftssamlingen benämnd ”Kringresande” som förts hos Polismyndigheten i Skåne med uppgifter om en stor mängd personer av romsk härkomst. I sin granskning av registret fann Säkerhets- och integritetsskyddsnämnden stora brister. Den allvarligaste bristen ansåg nämnden vara att ändamålet med personuppgiftsbehandlingen var alldeles för vitt. Visserligen föll det ändamål som åberopats, ”Länsövergripande brottslighet”, inom ramen för sådan underrättelseverksamhet som avses med det ändamål som anges i 2 kap. 7 § 1 polisdatalagen. Det uppfyllde dock inte det grundläggande kravet i 9 § första stycket c PuL – som också gäller vid behandling enligt polisdatalagen – på att insamling bara ska ske för särskilda, uttryckligt angivna och berättigade ändamål. Nämnden fortsatte enligt följande (uttalande 2013-11-15, dnr 173-2013).

> Ett oprecist ändamål ger inga ramar för personuppgiftsbehandlingen, vilket i praktiken sätter integritetsskyddet ur spel. Vidare är det klarlagt att det inte finns behov av att registrera alla de personer som finns i uppgiftsamlingen, inte ens med det vida ändamål som gällt. En annan allvarlig brist är att det inte finns ett tillräckligt tydligt samband mellan den av polismyndigheten angivna brottsligheten och de personuppgifter som behandlas. Sammantaget förefaller därför uppgiftssamlingen i vart fall delvis ha fått karaktären av en ”bra att ha”-uppgiftssamling.

Genom att i registerlagar ange mycket vida ändamål riskerar man alltså att tillämparen betraktar varje personuppgiftsbehandling som faller in under det i författning beskrivna ändamålet som en laglig

personuppgiftsbehandling eller, i vart fall, att varje begränsning i förhållande till lagens ändamålsbestämning är tillräcklig som ändamålsprecisering. Mot den bakgrunden menar vi att det kan ge ett i praktiken bättre integritetsskydd om den personuppgiftsansvarige är hänvisad enbart till att utifrån de grundläggande kraven i 9 § första stycket c på eget ansvar formulera ändamål som är tillräckligt specifika för att ge ledning för vilka uppgifter som är adekvata och inte för många för den aktuella behandlingen osv. Sådana mer specifika ändamålsbestämningar är vidare ägnade att underlätta för dels enskilda registrerade som vill kontrollera ändamålsenligheten i behandlingen av uppgifter om honom eller henne, dels tillsynsmyndighetens motsvarande kontroll.

Även när författningsreglerade ändamål är mer begränsade till sin utformning innefattar bestämningen ofta ett bemyndigande för den personuppgiftsansvariga myndigheten att behandla personuppgifter som behövs för att utföra en uppgift som myndigheten under alla förhållanden är ålagd att utföra enligt annan lagstiftning, myndighetsinstruktion, regeringsbeslut eller liknande. Något förenklat kan förhållandet beskrivas som att myndigheten enligt registerlagen får behandla de personuppgifter som myndigheten måste behandla i enlighet med vad som direkt eller indirekt följer av annan reglering som styr vilka uppgifter myndigheter har. Såvitt avser Skatteverket föreskrivs t.ex. i 1 kap. 4 § första stycket 2 lagen om behandling av uppgifter i Skatteverkets beskattningsverksamhet att verket får behandla uppgifter som behövs för det bestämmande av pensionsgrundande inkomst som Skatteverket samtidigt har ett åliggande att beräkna enligt 59 kap. SFB.

Som vi ser det är emellertid regler om vad myndigheter ska och får göra – och därmed vilken informationshantering som de behöver ägna sig åt – i grunden verksamhetsfrågor som inte hör hemma i dataskyddsregleringen utan bör regleras i annat sammanhang. En informationshanteringsförfattning bör enligt vår mening bara innehålla sådana bestämmelser som behövs därför att den insamlade informationen innehåller personuppgifter som hanteras elektroniskt – eller i manuella register – och därmed aktualiserar dataskyddsrättsliga frågor. Att genom ändamålsbestämningar styra vilka personuppgifter myndigheterna får samla in i sin verksamhet för att utföra sina åligganden innebär alltså ett slags dubbelreglering som inte alltid ter sig som en lämplig ordning.

Visserligen görs det genom ändamålsbestämningar tydligt för allmänhet och för registrerade inom vilka ramar myndigheter får samla in och behandla personuppgifter. Detta kan ha ett värde, särskilt när den reglering utifrån vilken myndigheter bedriver sin verksamhet är uppsplittrad på en mängd olika författningar och på skilda normnivåer. Information om vilken personuppgiftsbehandling som sker inom en viss myndighet kan emellertid mycket väl ges på annat sätt än genom författningsreglering. Vi återkommer till den frågan i kapitel 16.

Enligt vår mening kan det – bortsett från särskilt integritetskänslig behandling – ifrågasättas i vilken mån det egentligen är till gagn för registrerades personliga integritet med den ”dubbelreglering” som ges genom att först föreskriva att myndigheten ska göra något och sedan att den också får göra det. Till detta kommer att sådan dubbelreglering kan motverka effektiviteten i förvaltningen även när detta knappast är påkallat från integritetsskyddsynpunkt. Om en ny uppgift åläggs en myndighet och uppgiften ställer krav på personuppgiftsbehandling som inte redan faller in under en befintlig ändamålsbestämmelse, måste denna först ändras. Det kan vara en tämligen arbetskrävande och utdragen process eftersom ändamålsbestämmelser ofta har lagform. Såvitt vi har erfarit är det på inget sätt ovanligt att planerade nya effektivitetsfrämjande myndighetsövergripande samarbeten bromsas eller omöjliggörs därför att nödvändigt informationsutbyte förhindras på grund av att någon parts ändamålsbestämmelser inte är anpassade till den nya uppgiften. Ändamålsbestämmelser kan alltså föranleda tids- och resurskrävande lagstiftningsåtgärder även i situationer när detta inte framstår som särskilt angeläget från integritetsskyddssynpunkt.

Det är vidare vår uppfattning att frågan i vad mån en myndighet får lämna ut personuppgifter till andra myndigheter inte bör regleras genom ändamålsbestämmelser. Den diskussion som förekommit genom åren visar t.ex. att bestämmelser om s.k. sekundära ändamål ofta leder till tillämpningsproblem och osäkerhet angående förhållandet till andra bestämmelser, främst de i offentlighets- och sekretesslagen. Dessutom kan sekundära ändamål, som i realiteten ofta inte är uttömmande angivna, bidra till att uppgifter uppfattas vara i högre grad kringgärdade av restriktioner beträffande utlämnanden än vad som egentligen är fallet. Vi instämmer alltså i vad Integritetsskyddskommittén anfört om att utlämnande av uppgifter

till andra myndigheter inte bör regleras genom ändamålsbestämmelser. En helt annan sak är att det kan krävas bestämmelser som tillåter rutinmässigt utbyte av sekretessreglerade personuppgifter mellan myndigheter på sätt som ger stöd för att tillämpa den sekretessbrytande s.k. generalklausulen i 10 kap. 27 § OSL. Sådana bestämmelser bör dock, som vi redan har berört i avsnitt 5.7.2, inte rubriceras som eller i övrigt utformas som dataskyddsrättsliga ändamålsbestämmelser.

Sammanfattningsvis menar vi alltså att det finns avsevärda nackdelar förknippade med den regleringsmodell som hittills tillämpats och som inneburit att ändamålen – såväl primära som sekundära – ofta har författningsreglerats. Vi ser det inte som ändamålsenligt att den nya lagen skulle utgå från en huvudregel om att sådana bestämmelser ska finnas. Visserligen kan det inte uteslutas att det i specifika fall kan finnas en befogad anledning för lagstiftaren att genom ändamålsbestämningar reglera utrymmet när det gäller för vilka syften personuppgifter får behandlas. Det torde framför allt vara aktuellt beträffande personuppgifter i särskilt integritetskänsliga register eller andra uppgiftssamlingar. Exempelvis kan det vid direktåtkomst till sådana uppgiftssamlingar finnas anledning att genom för den mottagande myndigheten bindande bestämmelser reglera för vilka ändamål den ska få använda sin direktåtkomst genom att faktiskt överföra tillgängliga personuppgifter till sin verksamhet för läsning, nedladdning eller någon annan åtgärd som innebär en behandling i lagens mening. Sådana avgränsade ändamålsbestämmelser kan ges i den förordning som är avsedd att ansluta till den nya lagen eller, om det är lämpligare, i en särskild författning. I den mån det bedöms att lagform erfordras kan sådana bestämmelser tas in i en bilaga till den nya lagen. Valet kan bl.a. påverkas av var själva direktåtkomsten regleras, se vidare avsnitt 11.1 angående våra överväganden och förslag beträffande regleringen av direktåtkomst.

Mot bakgrund av det sagda är det vår samlade bedömning att den nya lagen inte bör innehålla några ändamålsbestämmelser eller förutsätta att sådana bestämmelser ska finnas. Vi föreslår därför inte någon sådan reglering. Vidare är det vår uppfattning att huvudregeln bör vara att ändamålen för myndigheters personuppgiftsbehandling inte bör särregleras i förhållande till den nya lagen.

Behandling av insamlade personuppgifter för nya ändamål

Bedömning: Finalitetsprincipen ska gälla då myndigheter behandlar personuppgifter med stöd av den generella lagen. Detta följer av hänvisningen till 9 § PuL.

Myndigheter kan bedriva sådan verksamhet där separata behandlingar sker för skilda ändamål eller för flera ändamål samtidigt. Finalitetsprincipen såsom den kommer till uttryck i 9 § första stycket d PuL ger utrymme för en rimlig flexibilitet hos personuppgiftsansvariga myndigheter utan att det i alltför hög grad sker på bekostnad av den registrerades intresse av att insamlade uppgifter om honom eller henne inte används i en oöverblickbar kedja av nya ändamål och sammanhang. Finalitetsprincipen såsom den kommer till uttryck i personuppgiftslagen bör alltså gälla även för myndigheter. Detta behöver inte regleras särskilt utan följer av hänvisningen till 9 § PuL. Den grundläggande regeln om att personuppgifter inte får behandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in blir därmed generellt tillämplig enligt den nya lagen.

Liksom normalt är fallet i dag, får det då behov uppstår inom den egna myndigheten av att behandla personuppgifter för nya ändamål göras en bedömning av om det nya ändamålet är oförenligt med de ursprungliga ändamål som fanns angivna då uppgifterna samlades in till myndigheten. Även om bedömningen blir att det nya ändamålet inte är oförenligt med det ursprungliga, så innebär det inte med självklarhet att behandlingen för det nya ändamålet är tillåten. Behandlingen för det nya ändamålet måste även vara nödvändig för att myndigheten ska kunna utföra en verksamhet som myndigheten ska eller får bedriva. Även de övriga grundläggande kraven i 9 § PuL måste iakttas. Personuppgifterna måste t.ex. vara adekvata och inte för många i förhållande till det nya ändamålet m.m.

När det gäller frågan om utlämnande av personuppgifter till andra myndigheter eller till enskilda är det alltså vår uppfattning att behandling i form av utlämnanden är förenliga med finalitetsprincipen så länge som utlämnandena som sådana sker i överensstämmelse med lag eller förordning enligt vilken uppgifterna får eller ska lämnas ut. Härmed avses i första hand utlämnanden till annan myndighet enligt 6 kap. 5 § OSL och utlämnanden av sekre-

tessreglerade uppgifter till en annan myndighet eller enskild, på begäran eller på eget initiativ, som sker med stöd av någon sekretessbrytande bestämmelse. Vi menar alltså att lagstiftaren genom att reglera ett uppgiftslämnande får anses ha tagit ställning till att sådana utlämnanden som ska eller får ske inte är oförenliga med ursprungliga ändamål. Myndigheterna är alltså bundna av den prövning enligt finalitetsprincipen som lagstiftaren gjort genom exempelvis en sekretessbrytande bestämmelse. I praktiken innebär detta att den nya lagen inte reglerar i vad mån personuppgifter får behandlas genom att lämnas ut från en myndighet så länge som utlämnandet sker i enlighet med offentlighets- och sekretesslagen eller bestämmelser i annan författning av innebörd att uppgifter får eller ska lämnas, på begäran eller självmant. En helt annan sak är att de krav som den nya lagen ställer på den personuppgiftsbehandling som själva utlämnandet innefattar givetvis ändå gäller, exempelvis kravet på adekvata säkerhetsåtgärder. Även vid sådana utlämnanden – liksom vid annan behandling av insamlade personuppgifter för icke oförenliga nya ändamål – måste vidare de grundläggande kraven i 9 § PuL iakttas. Det är t.ex. inte tillåtet vid ett enstaka fall av utlämnande på begäran av annan myndighet att lämna ut fler personuppgifter än vad som behövs för syftet med utlämnandet, dvs. att tillgodose mottagande myndighets begäran. Detta gäller alldeles oavsett om det kan leda till merarbete inom myndigheten att t.ex. sortera bort viss överflödig information före utlämnandet (9 § första stycket f PuL).

Tillämpningen av finalitetsprincipen ger således inte upphov till någon verklig – eller skenbar – konflikt mellan den nya lagen och sekretesslagstiftningen och bestämmelser i andra författningar som påbjuder eller tillåter uppgiftsutbyte. Vi har övervägt behovet av att klargöra detta genom en särskild föreskrift i den nya lagen men kommit till slutsatsen att detta inte behövs. Eftersom den nya lagen ska vara subsidiär till avvikande bestämmelser i annan lag eller förordning kommer bestämmelser i annan lag eller förordning om att utlämnanden ska eller får ske alltid att ha företräde.

Vilka personuppgifter får behandlas?

Bedömning: Utöver det slags personuppgifter för vilka dataskyddsdirektivet uppställer särskilda krav – känsliga personuppgifter, uppgifter om lagöverträdelser m.m. och personnummer eller samordningsnummer – bör det inte införas några regler om vilka personuppgifter som får eller inte får behandlas. Det grundläggande kravet på att inte fler personuppgifter än vad som är nödvändigt för ändamålet med behandlingen tillsammans med de övriga grundläggande kraven i 9 § PuL sätter gränsen för vilka personuppgifter som får behandlas.

Från integritetssynpunkt är det väsentligt att inte andra personuppgifter behandlas hos en myndighet än vad som är befogat utifrån myndighetens verksamhetsbehov. Dessa behov varierar i samma grad som det finns skillnader i myndigheternas verksamheter, dvs. i hög grad. Vi har emellertid ställt oss frågan om det finns skäl att – utöver det slags personuppgifter för vilka dataskyddsdirektivet uppställer särskilda krav, känsliga personuppgifter och uppgifter om lagöverträdelser m.m. – införa generella regler om vilket slags personuppgifter som myndigheter ska få behandla.

De grundläggande kraven enligt 9 § PuL innebär att insamling av uppgifter bara får ske för särskilda, uttryckliga och berättigade ändamål. De grundläggande kraven innebär vidare att personuppgifterna ska vara adekvata och relevanta i förhållande till ändamålen med behandlingen, att inte fler personuppgifter behandlas än vad som är nödvändigt med hänsyn till ändamålen med behandlingen samt att personuppgifter som behandlas ska vara riktiga och, om nödvändigt, aktuella. Hänvisningen till 9 § PuL innebär att de kraven kommer att gälla även vid behandling enligt den nya lagen. Att behandla ovidkommande eller onödigt många personuppgifter sett till de bestämda ändamålen är därmed olagligt. Dessa grundläggande krav innebär en såväl kvantitativ som kvalitativ begränsning i fråga om vilka personuppgifter som alls får behandlas inom en myndighet. Kan t.ex. en arbetsuppgift utföras tillfredsställande även med utlämnande av personuppgifter, t.ex. uppgifter om registrerades namn, är de grundläggande kraven i 9 § första stycket e och f inte uppfyllda, namnet behövs nämligen inte.

Prövningen av om en personuppgift är nödvändig för en viss behandling eller inte måste enligt vår mening göras kontinuerligt av myndigheterna och inte bara då uppgiften registreras eller på annat sätt samlas in i verksamheten. Även vid en senare hantering ska personuppgiften behövas för ändamålet med just den hanteringen. Det sagda innebär t.ex. att även om uppgiften om den registrerades namn med nödvändighet måste behandlas i handläggningen av ett ärende där den registrerade är part, så kanske namnuppgiften inte behövs vid en senare behandling t.ex. för att göra verksamhetsuppföljningar, i undervisningssammanhang eller för att informera allmänheten om principiellt viktiga avgöranden exempelvis genom att publicera dem på myndighetens webbplats. Det måste alltså vid sådan senare behandling alltid prövas om det går att utelämna personuppgifterna eller, i vart fall, att endast använda uppgifter som indirekt går att härleda till enskild person.

Enligt vår mening följer det av kraven enligt 9 § första stycket e, om adekvans och relevans i förhållande till ändamålen med behandlingen, samt f, om uppgiftsminimering, att myndigheter i så stor utsträckning som är möjligt använder personuppgifter som endast indirekt är hänförliga till den registrerade. Vi menar att detta också är förenligt med en rättssäker, effektiv och smidig förvaltning. I många sammanhang då sammanställd data tas fram för utförandet av en viss arbetsuppgift kan t.ex. olika former av kodning vara ett lämpligt sätt att skydda enskildas integritet.

I sammanhanget bör vidare erinras om att för det fall fullständig avidentifiering från verksamhetssynpunkt är ett fullgott alternativ till att använda direkta eller indirekta personuppgifter, är de lagliga förutsättningarna för att alls behandla personuppgifter utan den registrerades samtycke inte uppfyllda. Behandlingen behövs helt enkelt inte.

Som vi ser det innebär de grundläggande kraven enligt 9 § PuL en tillräcklig avgränsning i fråga om vilka slags personuppgifter myndigheter ska få behandla. Vi ser därmed inget behov av att införa några ytterligare regler om detta i den nya lagen.

En allmän och heltäckande rättslig grund för myndigheternas behandling av personuppgifter

Förslag: Bestämmelserna i 10 § a–f PuL om när behandling av personuppgifter är tillåten oberoende av samtycke ska inte tillämpas när myndigheter behandlar personuppgifter enligt den nya lagen. I stället införs en bestämmelse i lagen som innebär att en myndighet får behandla personuppgifter om det är nödvändigt för att myndigheten ska kunna utföra sin verksamhet.

Det är ett starkt allmänt intresse att myndigheterna ska kunna bedriva sina olika slags verksamheter på ett ändamålsenligt sätt, även om det innefattar elektronisk behandling av personuppgifter. Informationsteknikens genomslag på alla nivåer och i alla sammanhang medför att myndigheter i praktiken inte kan välja att behandla personuppgifter manuellt, i vart fall inte på ett sätt som inte omfattas av personuppgiftslagens regler. Det allmänna intresset av att myndigheternas verksamhet bedrivs effektivt och ändamålsenligt tillsammans med karaktären på myndigheternas verksamhet medför vidare att personuppgiftsbehandlingen knappast kan bygga på att registrerade lämnar sitt samtycke till behandlingen.

Artikel 7 i dataskyddsdirektivet innebär att medlemsstaterna ska föreskriva att personuppgifter får behandlas utan samtycke bara i de fall som anges i artikeln. Bestämmelsen i artikel 7 har i princip ordagrant implementerats genom 10 § PuL om när personuppgiftsbehandling är tillåten. Det står klart att artikel 7 i dataskyddsdirektivet på ett eller annat sätt måste genomföras även i den lag med en samlad reglering av myndigheters personuppgiftsbehandling som vi föreslår. Frågan är om detta, såsom beträffande 9 § PuL, bör ske genom en hänvisning till 10 § eller om det bör ske genom införandet av en reglering som ersätter den paragrafen, dvs. genom den metod som kan sägas vara den normala beträffande registerförfattningar.

De allmänt hållna bestämmelserna i 10 § PuL riktar sig till alla personuppgiftsansvariga oavsett om de är enskilda eller myndigheter och är bl.a. av den anledningen inte helt enkla att tillämpa på myndighetsområdet. Vi menar att en särskild bestämmelse med motsvarande innebörd i den generella lagen kan antas på ett bättre sätt tydliggöra och förenkla vad som ska gälla i fråga om när myn-

digheter får behandla personuppgifter. När det gäller utformningen av en sådan bestämmelse beaktar vi följande.

Varken en statlig eller kommunal myndighet kan på eget initiativ ta på sig nya uppgifter. Utgångspunkten är således att frågan om vilken personuppgiftsbehandling som behöver ske inom en viss myndighet styrs av vad myndigheten ålagts i form av uppgifter. Myndigheters verksamhet består emellertid inte enbart av aktiviteter som direkt går att identifiera såsom utförande av rättsliga skyldigheter, myndighetsutövning eller andra uppgifter och befogenheter som klart framgår av författning, regleringsbrev eller särskilda beslut. Varje myndighet har också ett ansvar för att planera, följa upp och kontrollera den egna verksamheten. En aktiv verksamhetsutveckling och kvalitetssäkring är vidare av mycket stor betydelse inom den offentliga sektorn och något som förväntas av alla myndigheter. Även i sådan verksamhet uppstår emellertid behov av att behandla personuppgifter. Ofta handlar det om analyser eller statistiska bearbetningar av uppgifter som redan har samlats in i myndighetens löpande verksamhet, men det kan också handla om insamling av uppgifter t.ex. genom enkäter m.m. Här kan också nämnas myndigheternas serviceverksamhet, kommunala medborgardialoger m.m. som bl.a. kan innebära aktiviteter som innefattar personuppgiftsbehandling. Nu nämnda exempel på aktiviteter är i normalfallet inte reglerade beträffande vad som ska utföras och hur det ska ske på samma sätt som är fallet beträffande myndigheternas ordinarie verksamheter. Det innebär dock inte att de sker i ett rättsligt vakuum. Den yttre ramen är givetvis det samband som alltid måste finnas med myndighetens grundläggande uppgifter och befogenheter.

Vissa myndigheter har utöver sina reglerade uppgifter också getts befogenheter att bedriva uppdragsverksamhet som kan innefatta försäljning av varor eller tjänster m.m. Detta framgår ofta av myndighetens instruktion, såsom är fallet t.ex. beträffande Statens fastighetsverk, E-hälsomyndigheten eller Skogsstyrelsen. Ett annat exempel är Lantmäteriet som har ålagts att försörja samhället med grundläggande information och därutöver getts befogenheter att bedriva uppdragsverksamhet i form av försäljning av olika tjänster. Forskningsverksamhet är en verksamhet som Folkhälsomyndigheten har getts befogenhet att bedriva medan det för andra myndigheter är ett åliggande, t.ex. för universitet och högskolor eller Brotts-

förebyggande rådet. Verksamhet av nu angivet slag kan regelmässigt också antas förutsätta att behandling av personuppgifter sker.

Till det sagda kommer reglering som direkt eller indirekt ålägger myndigheterna skyldigheter att registrera eller dokumentera information vari det med nödvändighet kan ingå personuppgifter, t.ex. generella bestämmelser såsom 5 kap. OSL om registrering av allmänna handlingar eller mer specifik reglering för olika myndigheter att utföra t.ex. viss dokumentering m.m. Alla myndigheter har vidare skyldigheter att tillhandahålla och bevara allmänna handlingar vilket som regel inbegriper behandling av personuppgifter.

Myndigheters verksamhet är således inte egeninitierad utan styrd både när det handlar om ålagda uppgifter och givna befogenheter. Vi föreslår mot den bakgrunden en bestämmelse som anger att en myndighet får behandla personuppgifter när det är nödvändigt för att myndigheten ska kunna utföra sin verksamhet. Härmed avses sådan verksamhet som en myndighet enligt det ovan sagda ska eller får bedriva. En sådan generell rättslig grund för myndigheters personuppgiftsbehandling är ägnad att i hög grad förenkla för myndigheterna när de ska bedöma om en viss personuppgiftsbehandling är tillåten eller inte samtidigt som den tydliggör för allmänheten vilken rätt myndigheterna har att behandla personuppgifter oberoende av de registrerades samtycke.

Enligt vår bedömning kan det inte råda någon tvekan om att en generell regel av angivet slag är förenlig med dataskyddsdirektivet. Som har framgått ovan råder det knappast något tvivel om att myndigheters verksamhet ryms under de olika punkterna i artikel 7 och den föreslagna bestämmelsen kan inte sägas innebära någon utvidgning i sak av vad som följer av den artikeln. Vad det är fråga om är behandling av personuppgifter som är nödvändig för att en arbetsuppgift av allmänt intresse eller som ett led i myndighetsutövning ska kunna utföras (artikel 7 e, jfr 10 § d och e PuL). Förutom att myndighetsverksamhet som ska eller får bedrivas är av allmänt intresse, sker informationshanteringen i verksamheten ofta som en följd av en rättslig förpliktelse (artikel 7 c, jfr 10 § b PuL). Den av oss föreslagna bestämmelsen kommer alltså sakligt sett inte att innebära någon förändring gentemot vad som skulle följa av en tillämpning av 10 § PuL.

För att en personuppgiftsbehandling ska vara tillåten räcker det emellertid inte med att myndigheten är ålagd eller har befogenhet

att utföra en viss verksamhet. Enligt artikel 7 i direktivet krävs också att det är nödvändigt att behandla personuppgifterna.

Vi har övervägt om nödvändighetsbegreppet, på motsvarande sätt som gjorts i flera informationshanteringsförfattningar, kunde ersättas av uttryckssättet att personuppgiftsbehandlingen ska behövas. På så sätt skulle obalansen i förhållande till begreppsanvändningen i offentlighets- och sekretesslagen kunna elimineras. I sekretesslagstiftningen används nämligen rekvisitet nödvändigt med en avsevärt mera snäv innebörd än vad som åsyftas med samma rekvisit i dataskyddsdirektivet. Enligt exempelvis 10 kap. 2 § OSL om nödvändigt utlämnande används rekvisitet nödvändigt för att tillämpningen av den sekretessbrytande bestämmelsen ska vara restriktiv och för att markera att det inte ska finnas utrymme för att tillämpa bestämmelsen för att motverka nedsatt effektivitet i myndighetens verksamhet. Men dataskyddsdirektivets och personuppgiftslagens nödvändighetsbegrepp är alltså avsevärt mera tillåtande. Det vore en god sak om man genom ett annat ordval kunde markera betydelseskillnaden mellan sekretesslagstiftningen och dataskyddsregleringen. Ordet nödvändig – ”necessary” i den engelska versionen – används emellertid i direktivet som ett självständigt unionsrättsligt begrepp (EU-domstolens dom den 16 december 2008 i mål C-524/06, Huber). Mot den bakgrunden anser vi inte att det finns utrymme att ersätta ordet nödvändig med ordet behövs eller något annat uttryck eftersom detta skulle riskera att leda till en tolkning som vore oförenlig med unionsrätten. Vi föreslår därför att begreppet nödvändig ska användas även i den nya lagen.

Med nödvändighetsrekvisitet avses detsamma som i 10 § PuL. Den närmare innebörden är således inte entydig. Som har framgått har det antagits att om en arbetsuppgift kan utföras nästan lika enkelt eller billigt med utelämnande av personuppgifter eller med personuppgifter som har avidentifierats, är rekvisitet inte uppfyllt (SOU 1997:39 s. 359). Viss vägledning ges vidare av EU-domstolens ovan nämnda dom i målet Huber. Till bilden hör vidare att det inte är helt oproblematiskt att särskilja frågorna om dels vilken behandling som är nödvändig för en verksamhet av visst slag, dels huruvida det grundläggande kravet att inte använda fler personuppgifter än vad som är nödvändigt för ändamålet med behandlingen är uppfyllt (9 § f PuL). Det är emellertid en svårighet som redan gäller vid en tillämpning av personuppgiftslagen och som

tycks vara inbyggd i dataskyddsdirektivet. Detta exemplifieras av Huber-domen där det t.ex. inte ansågs nödvändigt enligt artikel 7 e att behandla personuppgifter för statistikändamål. Den prövningen kan tyckas ligga nära det slags prövning som måste göras enligt principen om uppgiftsminimering enligt de grundläggande kraven. Frågeställningen om avgränsningen – eller rättare överlappningen – mellan nödvändighetskravet enligt den rättsliga grunden för myndigheters behandling som föreslås tas in i den nya lagen och de grundläggande kraven enligt 9 § PuL är alltså en generell företeelse som måste hanteras i rättstillämpningen. Det är också en överlappning som tycks leva vidare vid införandet av en kommande uppgiftsskyddsförordning. Enligt kommissionens förslag ska dels gälla som en princip om behandling av personuppgifter att ”personuppgifter bara ska behandlas om, och så länge som, syftena inte kan uppnås genom att man behandlar information som inte rör personuppgifter” (artikel 5 c), dels gälla att behandlingen, om den sker utan samtycke, ska vara nödvändig för vissa situationer (artikel 6.1 b–c).

Betydelsen av den registrerades inställning

Förslag: Det ska anges i den nya lagen att behandling av personuppgifter som är tillåten enligt lagen eller föreskrifter som meddelats i anslutning till lagen får utföras även om den enskilde motsätter sig behandlingen.

Vi föreslår alltså en grundläggande regel om att personuppgifter får – utan den registrerades samtycke – behandlas av en myndighet när det är nödvändigt för att myndigheten ska kunna utföra verksamhet som myndigheten ska eller får bedriva. Bestämmelsen ersätter 10 § PuL och är, som vi framhållit ovan, enligt vår mening förenlig med vad som sammantaget följer av artikel 7 b–f dataskyddsdirektivet.

I dataskyddsdirektivet tillmäts emellertid den enskilde registrerades inställning till personuppgiftsbehandling som regel en central och avgörande betydelse. Direktivet innehåller bestämmelser som berör frågor om verkan av att den enskilde registrerade dels samtycker till, dels motsätter sig en personuppgiftsbehandling. Genom artikel 7 åläggs medlemsstaterna att föreskriva att personuppgifter

får behandlas endast om den registrerade otvetydigt har lämnat sitt samtycke eller någon av de grunder för behandling utan samtycke som anges i b–f om nödvändig behandling är uppfyllda. Samtycke definieras i artikel 2 h som varje slag av frivillig, särskild och informerad viljeyttring genom vilken den registrerade godtar behandling av personuppgifter som rör honom. Enligt artikel 14 a i dataskyddsdirektivet ska den registrerade tillförsäkras rätten att – i vart fall då personuppgifter får behandlas utan samtycke därför att en arbetsuppgift av allmänt intresse skall kunna utföras eller i samband med myndighetsutövning eller efter en intresseavvägning (artikel 7 e och f, jfr 10 § d–f PuL) – ”när som helst av avgörande och berättigade skäl som rör hans personliga situation motsätta sig behandling av uppgifter som rör honom, utom när den nationella lagstiftningen föreskriver något annat” När invändningen är berättigad får den behandling som påbörjats av den registeransvarige inte längre avse dessa uppgifter.

Sverige har utnyttjat den möjlighet till undantag i den nationella lagstiftningen som ges i artikel 14 a. Enligt personuppgiftslagen har den registrerade bara getts en uttrycklig rätt att motsätta sig behandling för direkt marknadsföring, 11 § PuL, samt en rätt enligt 12 § PuL att återkalla ett lämnat samtycke då behandling av personuppgifter bara är tillåten med ett sådant samtycke enligt vissa angivna paragrafer. I övrigt kan den registrerade inte med rättslig verkan motsätta sig sådan behandling som är tillåten enligt 10 § personuppgiftslagen.

I särlagar i förhållande till personuppgiftslagen, främst informationshanteringsförfattningar, förekommer ibland bestämmelser som klargör att den registrerade inte med rättslig verkan kan motsätta sig den behandling av personuppgifter som är tillåten enligt lagen i fråga. Bestämmelserna har tillkommit mot bakgrund av att Lagrådet i några tidiga lagstiftningsärenden rörande särlagar för myndigheters behandling av personuppgifter förordade att bestämmelser skulle intas i lagarna som uttryckligen angav att den registrerade inte hade rätt att motsätta sig personuppgiftsbehandlingen enligt särlagarna, se t.ex. prop. 2000/01:33 s. 346 och lagen (2001:181) om behandling av uppgifter i Skatteverkets beskattningsverksamhet samt 114 kap. SFB rörande behandling av personuppgifter inom socialförsäkringens administration. Lagrådet, och senare även regeringen, har därvid åberopat ett behov av en uttrycklig reglering mot

bakgrund av vad artikel 14 a i dataskyddsdirektivet föreskriver om att den enskilde åtminstone i vissa fall skall garanteras en rätt att motsätta sig en personuppgiftsbehandling, om inte annat föreskrivs i nationell lagstiftning, se ovan.

Mera sällan förekommer reglering som klargör vad som gäller i fråga om huruvida den registrerades eventuella samtycke till en viss personuppgiftsbehandling i sig kan utgöra en legitim grund för behandlingen.

I 2 kap. 3 § patientdatalagen föreskrivs att behandling som inte är tillåten enligt lagen ändå får ske, med vissa undantag enligt angivna paragrafer i lagen, om den enskilde lämnat uttryckligt samtycke till behandlingen. Vidare föreskrivs att regeringen får meddela föreskrifter om att en behandling som inte är tillåten enligt lagen inte heller i andra fall får utföras trots att den enskilde uttryckligen samtyckt till behandlingen. I motiven till bestämmelsen anfördes bl.a. att paragrafen kan sägas ge uttryck för att en enskilds uttryckliga samtycke till en viss behandling av personuppgifter rörande honom eller henne normalt ska respekteras (prop. 2007/08:126 s. 227).

Av 7 § studiestödsdatalagen framgår att den enskilde kan samtycka till behandling för andra ändamål än de i lagen angivna ändamålen för behandling som är tillåten oavsett om den registrerade motsätter sig den. I motiven till bestämmelsen anfördes bl.a. att Centrala studiestödsnämnden redan erbjuder service av visst slag åt studiestödsberättigade. I den serviceverksamheten kan det finnas behov av att behandla registrerades personuppgifter för andra ändamål än dem som anges i studiestödsdatalagen. En förutsättning för den erbjudna servicen är att de registrerade samtycker till att deras personuppgifter behandlas för serviceändamålet. Enligt regeringen fanns det inget beaktansvärt integritetsskyddsintresse som talade mot att sådan behandling skulle få ske med stöd av den registrerades samtycke. Mot den bakgrunden fann regeringen vidare att det inte var nödvändigt med bestämmelser som förbjuder eller gör det möjligt att förbjuda behandling i studiestödsverksamheten som sker med den registrerades samtycke (prop. 2008/09:96 s. 47 f.).

När det gäller sådana informationshanteringsförfattningar som gäller i stället för personuppgiftslagen men där det hänvisas till bestämmelser i personuppgiftslagen som ska vara tillämpliga före-

kommer i gällande rätt ingen hänvisning till 10 § PuL, vare sig till samtyckesgrunden eller till grunderna för behandling utan samtycke. Inte heller brukar hänvisas till 15 § enligt vilken förbudet mot behandling av känsliga personuppgifter inte gäller om den registrerade uttryckligen samtyckt till behandlingen. Däremot hänvisas inte sällan till 34 § PuL enligt vilka den registrerades samtycke utgör laglig grund för överföring av personuppgifter till tredjeland. Ett exempel på det sagda är lagen om behandling av uppgifter i Skatteverkets beskattningsverksamhet. Såsom denna lag konstruerats torde det emellertid inte finnas något utrymme för Skatteverket att behandla personuppgifter med stöd av den enskildes samtycke om inte behandlingen ryms inom de ramar som ges i ändamålsregleringen i 1 kap. 4 och 5 §§.

Ska den registrerade kunna motsätta sig behandling?

Som vi redan har konstaterat kan myndigheternas informationshantering knappast göras beroende av att den registrerade samtycker till behandlingen. Inte heller bör den registrerade kunna motsätta sig behandlingen. Liksom i dag bör således gälla att den enskildes inte med stöd av dataskyddsregleringen ska kunna hindra en personuppgiftsbehandling som sker lagligen. Mot den bakgrunden bör det införas en bestämmelse som klargör att den registrerade inte kan motsätta sig en sådan behandling av personuppgifter som är tillåten enligt lagen. Utan en uttrycklig bestämmelse om detta är det nämligen tveksamt om regleringen kan anses utgöra en sådan nationell lagstiftning som krävs enligt artikel 14 a i dataskyddsdirektivet för att göra undantag från kravet på att enskilda ska garanteras en rätt att motsätta sig behandling som sker för att bl.a. utföra en arbetsuppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning. Av lagtekniska skäl bör detta framgå i en egen bestämmelse i den nya lagen snarare än genom en hänvisning till 12 § PuL.

Samtycke som rättslig grund för behandling?

Ett samtycke gör i princip alltid personuppgiftsbehandling tillåten enligt såväl dataskyddsdirektivet som personuppgiftslagen. En avgörande skillnad mellan samtycke och de övriga rättsliga grunderna för behandling är att det vid samtycke inte finns något nödvändighetsrekvisit. Vi har ställt oss frågan i vilken mån det kan finnas anledning att i den nya lagen föreskriva samtycke som rättslig grund för viss behandling. Om samtycke skulle vara en rättslig grund för myndigheters personuppgiftsbehandling skulle en myndighet inte behöva ta ställning till om personuppgiftsbehandlingen är nödvändig för att myndigheten ska kunna utföra sin verksamhet.

Man kan anta att det kommer att uppkomma situationer i myndigheternas verksamheter där det antingen anses etiskt lämpligt att inhämta den enskildes samtycke eller där detta behövs för att undanröja tveksamheter om behandlingen i fråga verkligen är nödvändig för att myndigheten ska kunna utföra sin verksamhet. Rena servicefunktioner kan vara exempel på detta. Många myndigheter är aktiva när det gäller att skapa och tillhandahålla elektronisk service för medborgarna, t.ex. e-tjänster eller andra serviceåtaganden som kan inbegripa personuppgiftsbehandling. Detsamma kan gälla för verksamhetsutveckling genom egeninitierad försöksverksamhet, bemötandeprojekt eller liknande som t.ex. kan inbegripa enkätundersökningar eller intervjuer och som myndigheterna visserligen utför inom ramen för sina verksamheter men som man inte är direkt ålagda att utföra. I den mån det är fråga om frivilligt deltagande kommer detta givetvis rent faktiskt bara att kunna äga rum med den registrerades samtycke. Huruvida samtycket också ska utgöra den rättsliga grunden för personuppgiftsbehandlingen är en helt annan sak.

Vi menar att det är av avgörande betydelse för förtroendet för myndigheternas verksamhet att utgångspunkten bör vara att myndigheterna dels bara behandlar personuppgifter när det är nödvändigt i dataskyddsrättslig mening, dels inte ägnar sig åt verksamhet som ligger utanför vad myndigheterna alls får göra. För det fall den registrerades otvetydiga samtycke skulle utgöra en rättslig grund för myndigheters behandling av personuppgifter skulle det ge en myndighet ett indirekt stöd för att samla in personuppgifter och bedriva verksamhet som det inte är meningen att myndigheten ska

ägna sig åt, vilket knappast är önskvärt. Det är en helt annan sak att myndigheterna inom ramen för sina respektive uppdrag har stor frihet att själva bestämma vad som ska göras och hur det ska ske när det t.ex. gäller sådana frågor som service, verksamhetsplanering och utveckling m.m.

Den generella rättsliga grunden som vi föreslagit ovan – att sådan behandling är tillåten som är nödvändig för att myndigheten ska kunna utföra sin verksamhet – hindrar inte att personuppgifter behandlas i samband med t.ex. e-tjänster, bemötandeprojekt eller vid myndigheters verksamhet i sociala medier. Däremot måste myndigheten, som vid alla andra aktiviteter, alltså ställa sig frågan om e-tjänsten, projektet osv. är en verksamhet som myndigheten får ägna sig åt. Dessutom måste den frågan ställas om personuppgiftsbehandlingen verkligen är nödvändig för aktiviteten i fråga. En ordning som innebär att myndigheterna skulle kunna behandla personuppgifter utan att det rent faktiskt är påkallat för bedrivandet av myndighetens verksamhet vore enligt vår mening från principiella synpunkter klart betänklig.

Det finns vidare skäl att betona att man måste skilja på frågan om rättslig grund för behandlingen av personuppgifter och på hur uppgifter rent faktiskt kan eller får samlas in. Även om en viss personuppgiftsbehandling i och för sig är tillåten innebär det inte att uppgifter får samlas in med tvång. Insamlandet kan förutsätta den registrerades frivilliga medverkan och eget uppgiftslämnande eller att myndigheten har givits rätt att inhämta uppgifterna från annan myndighet eller enskild, t.ex. en arbetsgivare. Frågor som t.ex. uppgiftsskyldighet för enskilda ska regleras i anslutning till regleringen av respektive sakverksamhet och har inget samband med samtycke som rättslig grund för personuppgiftsbehandling. Såvitt avser t.ex. e-tjänster innebär detta att tvångsanslutning förutsätter författningsstöd i något slags verksamhetsreglering.

Mot bakgrund av det sagda menar vi att den registrerades samtycke inte bör vara en självständig rättslig grund för myndigheters behandling av personuppgifter enligt den nya lagen. Vi föreslår alltså ingen sådan regel. Det innebär principiellt sett en förändring i förhållande till gällande rätt, i vart fall såvitt avser den behandling som inte är särreglerad i registerförfattningar utan som stöder sig på personuppgiftslagen. Det praktiska behovet av samtycke som enda rättsliga grund för myndigheters personuppgiftsbehandling torde

emellertid vara obetydligt, varför vi inte ser att detta kommer att leda till några olägenheter.

Det kan tyckas som om dataskyddsdirektivet ovillkorligen kräver att även artikel 7 a om samtycke måste genomföras i all lagstiftning rörande personuppgiftsbehandling som omfattas av direktivets tillämpningsområde. Direktivet är emellertid i allt väsentligt inriktat på att skapa en dataskyddsreglering som åstadkommer ett harmoniserat integritetsskydd inom unionen vad gäller enskilda aktörers behandling av personuppgifter för att på så sätt möjliggöra ett fritt utbyte av personuppgifter över nationsgränserna. Visserligen omfattas även myndigheter av direktivet. Vi kan dock inte se det som stridande mot direktivet att beträffande den offentliga sektorn avstå från att föreskriva samtycke som rättslig grund. Det kan knappast sägas att Sverige därmed avviker från direktivet genom att skapa ett bättre eller sämre integritetsskydd än vad direktivet innebär. Inte heller kan det förhållandet att samtycke inte ska vara rättslig grund för myndigheters personuppgiftsbehandling rimligen verka hindrande för det fria flödet av personuppgifter mellan medlemsstaterna.

9.3 Tillåten behandling av särskilda kategorier av personuppgifter

9.3.1 Känsliga personuppgifter

Allmänna dataskyddsrättsliga regler

Dataskyddsdirektivet

Enligt artikel 8.1 i dataskyddsdirektivet ska medlemsstaterna förbjuda behandling av personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening samt uppgifter som rör hälsa och sexualliv.

I artikel 8.2 föreskrivs undantag från förbudet att behandla de uppgifter som avses i 8.1. Dessa rör om

a) den registrerade lämnat sitt uttryckliga samtycke till sådan behandling, utom i de fall medlemsstatens lagstiftning säger att samtycke inte kan upphäva förbudet i punkt 1,

b) behandlingen är nödvändig för att fullgöra de skyldigheter och särskilda rättigheter som åligger den registeransvarige inom arbetsrätten, i den omfattning detta är tillåtet enligt en nationell lagstiftning som föreskriver lämpliga skyddsåtgärder, eller

c) behandlingen är nödvändig för att skydda den registrerades eller någon annan persons grundläggande intressen när den registrerade är fysiskt eller rättsligt förhindrad att ge sitt samtycke, eller

d) behandlingen utförs inom ramen för berättigad verksamhet hos en stiftelse, en förening eller ett annat icke vinstdrivande organ, som har ett politiskt, filosofiskt, religiöst eller fackligt syfte, förutsatt att behandlingen endast rör sådana organs medlemmar eller personer som på grund av organets ändamål har regelbunden kontakt med detta och uppgifterna inte lämnats ut till tredje man utan den registrerades samtycke, eller

e) behandlingen rör uppgifter som på ett tydligt sätt offentliggörs av den registrerade eller är nödvändiga för att kunna fastslå, göra gällande eller försvara rättsliga anspråk.

Vidare sägs i artikel 8.3 att punkt 1 inte gäller när behandlingen av uppgifterna är nödvändig med hänsyn till förebyggande hälso- och sjukvård, medicinska diagnoser, vård eller behandling eller administration av hälso- eller sjukvård eller när dessa uppgifter behandlas av någon som är yrkesmässigt verksam på hälso- och sjukvårdsområdet och som enligt nationell lagstiftning eller bestämmelser som antagits av behöriga nationella organ är underkastad tystnadsplikt eller av en annan person är ålagd en liknande tystnadsplikt.

Enligt artikel 8.4 får medlemsstaterna antingen i sin nationella lagstiftning eller genom beslut av tillsynsmyndigheten besluta om andra undantag än de som nämns i punkt 2. Som förutsättningar gäller att det finns lämpliga skyddsåtgärder och att det sker av hänsyn till ett viktigt allmänt intresse.

Personuppgiftslagen m.m.

Bestämmelserna i artikel 8.1–8.4 dataskyddsdirektivet har genomförts i svensk rätt genom 13–20 §§ PuL. De uppgifter som avses i artikel 8.1 betecknas i personuppgiftslagen som känsliga personuppgifter (13 § tredje stycket).

Direktivets bestämmelser har i sak oförändrade förts över till personuppgiftslagen. Det generella förbudet mot behandling av känsliga personuppgifter finns i 13 §. I 14 § första stycket finns endast en upplysning om att det finns undantag från förbudet i 13 § i de fall som anges i 15–19 §§. I 15 § finns en bestämmelse som tillåter behandling vid samtycke och efter den registrerades tydliga offentliggörande, i 16 § anges de fall av nödvändig behandling som avses i artikel 8.2 a–c, undantaget för ideella organisationer m.fl. finns i 17 § och för hälso- och sjukvård i 18 §.

I 19 § har den svenske lagstiftaren utnyttjat möjligheten enligt 8.4 i direktivet att i nationell lagstiftning medge undantag från förbudet att behandla känsliga personuppgifter med hänsyn till ett viktigt allmänt intresse. Genom bestämmelsen tillåts att sådana uppgifter, under vissa förutsättningar, får behandlas för forskningseller statistikändamål. I förarbetena anförde regeringen att forskning och statistik är så viktiga områden att de borde regleras redan i den nya lagen (prop. 1997/98:44 s. 70).

Genom 20 § bemyndigas regeringen eller den myndighet som regeringen bestämmer att meddela ytterligare undantag från förbudet i 13 §, om det behövs med hänsyn till ett viktigt allmänt intresse. Uttrycket viktigt allmänt intresse avses ha samma innebörd som enligt artikel 8.4 i direktivet (prop. 1997/98:44 s. 129).

Om känsliga personuppgifter behandlas på så sätt att de inte ingår i eller är avsedda att ingå i en samling av personuppgifter som har strukturerats för att påtagligt underlätta sökning efter eller sammanställning av personuppgifter, är behandlingen tillåten enligt den s.k. missbruksregeln i 5 a § som innebär undantag från flera av lagens hanteringsregler. Det gäller under förutsättning att behandlingen inte innebär en kränkning av den registrerades personliga integritet.

Bemyndigandet i 20 § har utnyttjats av regeringen genom att det i 8 § PuF har införts en bestämmelse som föreskriver att det, utöver vad som följer av 5 a § och 15–19 §§ PuL, är tillåtet för myn-

digheter att behandla känsliga personuppgifter i löpande text om uppgifterna har lämnats i ett ärende eller är nödvändiga för handläggningen av det.

Förslaget till uppgiftsskyddsförordning

Även i kommissionens förslag till uppgiftsskyddsförordning finns i artikel 9.1–9.3 särskilda bestämmelser om när behandling av känsliga personuppgifter är tillåten. Bestämmelserna är utformade på grundval av motsvarande regler i dataskyddsdirektivet och avser samma typer av uppgifter, dock med tillägg för genetiska uppgifter. Också förordningen innehåller ett principiellt förbud mot behandling av sådana uppgifter. Nu gällande undantagsgrunder återfinns i förslaget. Därutöver har en ny grund tillkommit. Det rör undantaget som tillåter behandling enligt artikel 9.2 i som rör personuppgifter som är nödvändig för historiska, statistiska eller vetenskapliga forskningsändamål med förbehåll för de villkor och skyddsåtgärder som avses i artikel 83.

I artikel 9.2 g finns förslag till ett undantag som motsvarar det som nu finns i artikel 8.4 i dataskyddsdirektivet och som är av särskilt intresse såvitt avser myndigheters verksamhet. Enligt förslaget är behandling av känsliga personuppgifter tillåten om den är nödvändig för att genomföra en arbetsuppgift som utförs i allmänhetens intresse, på grundval av unionslagstiftningen eller en medlemsstats lagstiftning som ska innehålla bestämmelser om lämpliga åtgärder för att säkerställa den registrerades berättigade intressen. Det krävs alltså inte längre att det ska vara fråga om ett viktigt allmänt intresse, utan det räcker med att det finns ett allmänintresse för att undantag ska kunna göras. Vidare nämns inte längre uttryckligen att tillsynsmyndigheten får besluta om undantag.

I den svenska översättningen görs en kommatering som ger intryck av att det är fråga om en uppräkning, dvs. att behandling får ske dels om den är nödvändig för att genomföra en arbetsuppgift som utförs i allmänhetens intresse, dels på grundval av unionslagstiftningen eller en medlemsstats lagstiftning. Den engelska versionen ger emellertid intryck av att det ska vara fråga om en behandling som utförs i allmänhetens intresse på grundval av antingen unionslagstiftningen eller en medlemsstats lagstiftning.

Enligt förslaget till artikel 9.3 ska kommissionen ha befogenhet att anta delegerade akter enligt artikel 86 i syfte att närmare precisera kriterierna, villkoren och de lämpliga skyddsåtgärderna för behandlingen av de särskilda kategorier av personuppgifter som avses i punkt 1 och de undantag som fastställs i punkt 2.

I Europaparlamentets resolution med ändringsförslag föreslås att det alltjämt ska krävas att det är frågan om ett ”viktigt” allmänt intresse för att ett undantag ska vara tillåtet. Parlamentet föreslår också tillägg i uppräkningen av vilka uppgifter som ska omfattas, bl.a. ifråga om uppgifter om sexuell läggning och biometriska uppgifter.

Några kommentarer

Det kan konstateras att såväl dataskyddsdirektivet som förslaget till uppgiftsskyddsförordning medger att det införs lagstiftning som tillåter behandling av känsliga personuppgifter om det behövs med hänsyn till ett allmänt intresse. Enligt direktivet krävs vidare att det är fråga om ett viktigt allmänt intresse. I kommissionens förslag till uppgiftsskyddsförordning finns emellertid inte något krav på att allmänintresset ska vara viktigt.

Som ytterligare förutsättningar gäller enligt direktivet och förslaget till förordning att en tillåtelse att behandla känsliga personuppgifter ska förenas med lämpliga åtgärder för att skydda den registrerades berättigade intressen.

Det kan konstateras att uppgiftsskyddsförordningen, till skillnad från dataskyddsdirektivet, inte är lika tydlig med på vilket sätt en undantagssituation ska manifesteras. Enligt direktivet är det tydligt att ett undantag förutsätter att det beslutats om ett sådant genom antingen lagstiftning eller beslut av tillsynsmyndigheten. Av förordningen framgår inte lika tydligt vad det är som ska framgå av antingen unionslagstiftningen eller en medlemsstats lagstiftning, dvs. om det är undantaget eller om det är den arbetsuppgift av allmänt intresse som kräver behandling av känsliga personuppgifter för sitt fullgörande som kan motivera ett undantag.

Våra överväganden och förslag

Förslag: Utöver vad som följer av 15, 16, 18 och 19 §§ PuL – vilka paragrafer den nya lagen ska hänvisa till som tillämpliga på motsvarande sätt vid personuppgiftsbehandling enligt lagen – tillåts myndigheter att behandla känsliga personuppgifter om uppgifterna har lämnats i ett ärende eller är nödvändiga för handläggning av det. I annan verksamhet får känsliga personuppgifter behandlas endast i löpande text.

Regeringen eller den myndighet som regeringen bestämmer bemyndigas att medge ytterligare undantag, om det behövs med hänsyn till ett viktigt allmänt intresse.

Nuvarande författningsstöd för myndigheters behandling av känsliga personuppgifter

Enligt dataskyddsdirektivet gäller alltså speciella regler för särskilda kategorier av uppgifter. En sådan kategori är det slag av uppgifter som i personuppgiftslagen betecknas som känsliga personuppgifter. Enligt direktivet är det som huvudregel förbjudet att behandla sådana uppgifter. Ett sådant förbud har därför införts genom 13 § PuL.

Som framgått är det emellertid tillåtet att behandla känsliga personuppgifter om den registrerade har lämnat sitt samtycke till behandlingen eller det är fråga om vissa särskilda situationer som räknas upp i artikel 8.2–8.3 i direktivet. Motsvarande undantag har införts i 15–19 §§ PuL. Det kan konstateras att dessa särskilda undantagsfall inte på långa vägar ger möjlighet för myndigheter att behandla känsliga personuppgifter i alla de situationer då en sådan behandling kan vara nödvändig. Myndigheters möjlighet att behandla personuppgifter kan inte heller göras beroende av att den enskilde ger sitt samtycke till behandlingen. Det finns därför ett behov av att på myndighetsområdet ge möjlighet att, oavsett av om det finns samtycke från enskilde, behandla känsliga personuppgifter även i andra fall än de som särskilt räknas upp i dataskyddsdirektivet.

Enligt artikel 8.4 i direktivet finns det möjlighet att medge ytterligare undantag från förbudet att behandla känsliga personuppgifter av hänsyn till ett viktigt allmänt intresse. I en mängd registerlagar

medges med stöd av undantaget i direktivet och 2 § PuL behandling av känsliga personuppgifter på aktuella myndighetsområden. Genom 20 § PuL bemyndigas regeringen eller den myndighet som regeringen bestämmer att meddela föreskrifter om sådana undantag. Generellt tillämpliga bestämmelser har också meddelats på förordningsnivå med stöd av det bemyndigandet. Enligt 8 § PuF tillåts myndigheter att – utöver vad som följer av 5 a och 15–19 §§ PuL – behandla känsliga personuppgifter i löpande text, om uppgifterna har lämnats i ett ärende eller är nödvändiga för handläggningen av det. Som framgått har det med stöd av direktivets möjlighet till undantag även införts bestämmelser i 19 § PuL som tillåter behandling av känsliga personuppgifter för forsknings- eller statistikändamål. Dessa bestämmelser gäller för både myndigheter och enskilda.

För en myndighet som behandlar personuppgifter enbart med stöd av personuppgiftslagen och det inte är fråga om en sådan behandling som avses i 15–19 §§ PuL eller 8 § PuF, kan således 5 a § PuL ge ett visst ytterligare utrymme för att behandla känsliga personuppgifter. Av förarbetena till bestämmelsen framgår emellertid att syftet med denna undantagsbestämmelse knappast var att underlätta myndigheters behandling av personuppgifter. Det följer emellertid uttryckligen av utformningen av 8 § PuF att stadgandet i 5 a § PuL är tillämpligt även för myndigheterna (se vidare övervägandena i avsnitt 8.3.2 om behovet av en regel motsvarande 5 a § PuL på myndighetsområdet).

Det finns behov av ett generellt undantag som i tillräcklig utsträckning tillåter myndigheter att behandla känsliga personuppgifter

Mot bakgrund av betydelsen av en väl fungerande förvaltning är det enligt vår uppfattning ett viktig allmänt intresse att myndigheter kan behandla de känsliga personuppgifter som förekommer i deras verksamhet, oavsett hur uppgifterna har hamnat där, och att myndigheterna kan behandla dem på samma sätt som de i övrigt behandlar personuppgifter. Samtidigt indikerar direktivets krav på att det ska vara frågan om ett viktigt allmänt intresse att en tillåtande bestämmelse ska ges en restriktiv utformning och ha som utgångspunkt att kravet på nödvändighet för att det ska vara tillåtet att behandla känsliga personuppgifter bör vara större än vad som gäller i fråga om personuppgifter som inte är känsliga.

En bestämmelse som generellt medger att myndigheter får behandla känsliga personuppgifter bör därför ges en sådan utformning att den motsvarar ett minsta möjliga gemensamma behov hos myndigheterna av att behandla sådana personuppgifter.

Det kan konstateras att det i princip förekommer eller i vart fall kan förekomma känsliga personuppgifter i all myndighetsverksamhet. På en del verksamhetområden är behovet av att behandla känsliga personuppgifter stort, exempelvis inom socialförsäkringen, hälso- och sjukvården och socialtjänsten. På andra områden är behovet betydligt mindre och någon insamling för egen del av känsliga personuppgifter sker därför inte, eftersom det inte behövs för att hantera myndighetens ärenden. Parter i ärenden hos sådana myndigheter kan emellertid själva uppge känsliga personuppgifter – exempelvis uppgifter om hälsa – i sina inlagor till myndigheten. Det ligger således i dessa fall delvis utanför myndighetens kontroll om känsliga personuppgifter förekommer i verksamheten eller inte. En myndighet bör i ett sådant fall inte vara hänvisad till att behandla dessa uppgifter på ett annat sätt än det som annars gäller beträffande myndighetens verksamhet, dvs. exempelvis genom att endast dokumentera eller bevara uppgifterna i pappersform. Det kan alltså konstateras att alla myndigheter har behov av att automatiserat kunna behandla även känsliga personuppgifter.

Dataskyddsdirektivet kräver att förbudet mot att behandla sådana uppgifter i princip även gäller på myndighetsområdet. Det principiella förbudet enligt 13 § PuL mot att behandla känsliga personuppgifter måste således gälla även för myndigheter. En hänvisning till den bestämmelsen bör därför göras i den nya lagen. Det behövs emellertid ett generellt undantag som i erforderlig utsträckning medger sådan behandling utöver vad som följer av de särskilda undantagsfall som kan bli aktuella att tillämpa på myndighetsområdet (15, 16, 18 och 19 §§ PuL).

Det generella undantag för myndigheters behandling av känsliga personuppgifter som finns i 8 § PuF är begränsat på så sätt att det endast tar sikte på behandling i löpande text. Det tillåter vidare endast behandling av uppgifter som har lämnats i ett ärende eller är nödvändiga för handläggningen av det. Det kan konstateras att bestämmelsen således inte tillåter den behandling av känsliga personuppgifter som kan förekomma i en myndighets verksamhet som inte utgör ärendehandläggning, dvs. s.k. faktisk verksamhet. Det

kan exempelvis handla om rådgivning och annan service, uppföljning eller olika former av samverkan utan ärendeanknytning mellan myndigheter eller i förhållande till enskilda.

Det behov som i övrigt kan finnas eller uppstå av att behandla känsliga personuppgifter inom olika myndigheter får antas ha hämtat sitt stöd i undantagsbestämmelsen i 5 a § PuL, såvida inte någon tillämplig särreglering föreligger. Den bestämmelsen har emellertid inte införts i syfte att underlätta myndigheters behandling av personuppgifter. Det torde vidare i praktiken vara mycket svårt för en myndighet att avgöra om dess behandling av känsliga personuppgifter riskerar att utgöra en kränkning av den registrerades personliga integritet i den mening som avses i 5 a § PuL. Det kan därför varken med hänsyn till behovet av en fungerande verksamhet hos myndigheterna eller till den enskildes rätt till skydd för sina personuppgifter anses tillfredsställande att myndigheterna i sista hand måste förhålla sig till denna bestämmelse då det uppstår ett behov av att behandla känsliga personuppgifter som inte kan uppfyllas inom ramen för övriga bestämmelser. Vi anser därför att det finns ett tydligt behov av att i den nya lagen införa en bestämmelse som generellt tillåter behandling av känsliga personuppgifter i större omfattning än vad det nuvarande generella undantaget i 8 § PuF innebär. En sådan generellt tillåtande bestämmelse kan också i väsentlig mån bidra till att minska behovet av att genom särreglering på olika myndighetsområden tillåta sådan behandling.

Den omständigheten att myndigheter automatiserat behandlar de känsliga personuppgifter som de behöver för att kunna utföra sina uppgifter kan i normalfallet inte i sig anses utgöra något sådant ingrepp i enskilds personliga förhållanden som avses i 8 kap. 2 § andra stycket 2 RF och som i så fall kräver stöd i lag. Utgångspunkten är således att bestämmelser av detta slag i normalfallet ligger inom regeringens primärområde och därför kan meddelas i förordning. Genom en bestämmelse i den nya lagen som i viss begränsad utsträckning tillåter att myndigheter behandlar känsliga personuppgifter ges emellertid ett stöd i lag i den mån detta krävs enligt 8 kap. 2 § andra stycket 2 RF.

Känsliga personuppgifter i ärenden

Myndigheter bör generellt tillåtas att behandla känsliga personuppgifter som har lämnats i ett ärende eller är nödvändiga för handläggningen av det. I de fall känsliga personuppgifter förekommer i en inlaga som har lämnats till myndigheten i ett ärende som den handlägger kan det knappast krävas att det är nödvändigt att myndigheten behandlar uppgiften. Myndigheten saknar ju kontroll över vilka uppgifter som förekommer i inlagor som kommer in till den, men har samtidigt ett behov av att kunna hantera en inlaga även om myndigheten inte har något behov av att i ett senare skede behandla de känsliga personuppgifter som kan finnas där. I den mån känsliga personuppgifter behöver behandlas av annat skäl, exempelvis på grund av att myndigheten själv har samlat in uppgiften, bör det emellertid krävas att det är nödvändigt att den känsliga personuppgiften behandlas i ärendet. Frågan om det är nödvändigt att behandla uppgiften får därmed avgöras med hänsyn till vilken typ av ärende det är frågan om.

Bestämmelsen i 8 § PuF som generellt tillåter myndigheter att behandla känsliga personuppgifter är begränsad på så sätt att den bara är tillämplig på ärendehandläggning. Den är också begränsad såtillvida att den bara tillåter behandling av sådana uppgifter i löpande text.

Det kan konstateras att myndigheters ärenden i dag vanligen hanteras inom ramen för ett elektroniskt ärendehanteringssystem, dvs. annorlunda uttryckt i en databas. Som exempel på databaser som bl.a. innehåller ärendehanteringssystem kan nämnas beskattningsdatabasen och socialförsäkringsdatabasen. I den mån det i myndigheters ärendedokumentation finns känsliga personuppgifter behöver de alltså kunna behandlas i ärendehanteringssystemen inte bara om de förekommer i löpande text. En bestämmelse som generellt tillåter myndigheter att behandla känsliga personuppgifter bör således tillåta hantering av känsliga personuppgifter inom ramen för ett ärendehanteringssystem oavsett om de förekommer i löpande text eller inte. Myndigheters möjlighet att behandla känsliga personuppgifter vid handläggning av ärenden kan därför inte begränsas till löpande text.

Genom att personuppgifter samlas i ett system som innebär att de blir tillgängliga även utanför de enskilda ärendena kan det finnas

tekniska möjligheter att göra sammanställningar eller bearbeta informationen på annat sätt. Den särskilda risk för skyddet av känsliga personuppgifter som kan anses uppstå genom att uppgifterna samlas på detta sätt och görs möjliga för bearbetning får motverkas bl.a. genom att det införs sökbegränsningar. Vi återkommer till den frågan i avsnitt 9.4.

Känsliga personuppgifter i annan verksamhet

Myndigheters verksamhet består inte endast av handläggning av ärenden. Även annan verksamhet förekommer, såsom exempelvis rådgivning och annan service, uppföljning och olika former av samverkansprojekt. Känsliga personuppgifter kan behöva behandlas också i sådan verksamhet. I vilken utsträckning sådan verksamhet förekommer hos myndigheterna går inte att beskriva på något enhetligt sätt. Det kan dock konstateras att s.k. faktisk verksamhet torde förekomma i någon mån hos alla myndigheter och kan t.o.m. vara den dominerande inom vissa myndighetsområden, exempelvis inom utbildningsväsendet. Enligt vår uppfattning har den generellt tillåtande bestämmelse som för myndigheternas del redan finns i 8 § PuF, därför en alltför begränsad utformning för att kunna uppfylla ett minsta möjliga behov av att behandla känsliga personuppgifter på myndighetsområdet. Vi anser därför att en bestämmelse som generellt tillåter myndigheter att behandla känsliga personuppgifter också bör kunna tillämpas på annan verksamhet än ärendehandläggning. Den generellt tillåtande bestämmelsen bör i denna del emellertid vara begränsad till behandling av känsliga personuppgifter i löpande text. Enligt vår uppfattning kan man däremot inte motivera att det med hänsyn till ett viktigt allmänt intresse finns ett behov hos alla myndigheter att i verksamhet som inte utgör handläggning av ärenden bygga upp datoriserade uppgiftssamlingar, exempelvis i form av regelrätta register eller databaser, där känsliga personuppgifter får registreras i strukturerad form. I viss sådan myndighetsverksamhet kan det däremot finnas ett sådant behov. Detta förutsätter i så fall särskild reglering.

Med den utformning som nu föreslås för en bestämmelse som generellt tillåter myndigheter att behandla känsliga personuppgifter

torde det inte finnas något kvarstående behov av ett undantag motsvarande 5 a § PuL för att sådan behandling ska vara möjlig.

Ytterligare behov av att behandla känsliga personuppgifter får regleras särskilt

I den mån det finns andra behov hos vissa myndigheter av att få behandla känsliga personuppgifter som inte kan uppfyllas inom ramen för den generella bestämmelse som nu föreslås, får det i sådant fall ske genom särskilda bestämmelser. Det kan då ske genom särreglering som i större utsträckning än den generella lagen tillåter behandling av känsliga personuppgifter hos en viss myndighet eller inom ett visst verksamhetsområde.

I 20 § PuL ges regeringen eller den myndighet som regeringen bestämmer bemyndigande att meddela föreskrifter om ytterligare undantag, utöver 15–19 §§, från förbudet i 13 § mot att behandla känsliga personuppgifter om det behövs med hänsyn till ett viktigt allmänt intresse. Enligt vår uppfattning bör ett liknande bemyndigande införas i den nya lagen. En myndighets behov av att behandla känsliga personuppgifter som inte kan uppfyllas genom den generella bestämmelsen kan därmed regleras särskilt både på lag- och förordningsnivå eller i form av en myndighetsföreskrift.

Avslutningsvis kan noteras att det inte är självklart att ett sådant bemyndigande är förenligt med den föreslagna utformningen av artikel 9.2 g i uppgiftsskyddsförordningen. Enligt den föreslagna artikeln ska en behandling av känsliga personuppgifter vara tillåten på grundval av unionslagstiftningen eller en medlemsstats lagstiftning. Till skillnad från artikel 8.4 i dataskyddsdirektivet föreslås således ingen uttrycklig hänvisning till att en medlemsstats tillsynsmyndighet kan besluta om undantag från förbudet att behandla känsliga personuppgifter med hänsyn till ett allmänt intresse. Som redan påpekats är det frågan om förordningen över huvud taget anbefaller att det ska beslutas om ett undantag. Texten kan också tolkas så att det är själva den arbetsuppgift av allmänt intresse som kan motivera ett undantag som ska framgå av lagstiftning inom antingen unionen eller medlemsstaten.

Kommissionens förslag till uppgiftsskyddsförordning innehåller inte heller, till skillnad från dataskyddsdirektivet, något krav på att ett undantag från förbudet att behandla känsliga personuppgifter

behövs med hänsyn till ett viktig allmänt intresse, utan det räcker med att det är frågan om ett allmänt intresse. EU-parlamentet har i sin resolution med ändringsförslag emellertid föreslagit att det alltjämt ska finnas ett krav på att det frågan om ett viktigt allmänt intresse. I nuläget är det oklart vilket krav som kommer att ställas för att ett undantag ska vara tillåtet.

I avvaktan på att det bringas klarhet i nämnda frågor föreslår vi inte någon alternativ utformning av den aktuella bestämmelsen med hänsyn till en kommande uppgiftsskyddsförordning, utan utgår från att lagen även på sikt kan innehålla såväl ett krav på att det ska vara frågan om ett viktigt allmänt intresse som ett bemyndigande i denna del.

9.3.2 Personuppgifter om lagöverträdelser m.m.

Allmänna dataskyddsrättsliga regler

Dataskyddsdirektivet

Enligt artikel 8.5 i dataskyddsdirektivet får behandling av uppgifter om lagöverträdelser, brottsmålsdomar eller säkerhetsåtgärder utföras endast under kontroll av en myndighet eller – om lämpliga skyddsåtgärder finns i nationell lag – med förbehåll för de ändringar som medlemsstaterna kan tillåta med stöd av nationella bestämmelser som innehåller lämpliga och specifika skyddsåtgärder. Ett fullständigt register över brottmålsdomar får dock föras endast under kontroll av en myndighet.

Medlemsstaterna får föreskriva att uppgifter som rör administrativa sanktioner eller avgöranden i tvistemål också ska behandlas under kontroll av en myndighet.

Personuppgiftslagen m.m.

Bestämmelserna i artikel 8.5 har genomförts i svensk rätt på så sätt att det genom 21 § första stycket PuL har införts ett förbud för andra än myndigheter att behandla personuppgifter om lagöverträdelser som innefattar brott, domar i brottmål, straffprocessuella tvångsmedel eller administrativa frihetsberövanden.

Enligt 21 § andra stycket PuL tillåts att andra än myndigheter behandlar sådana personuppgifter som avses i första stycket för forskningsändamål, om behandlingen har godkänts enligt lagen (2002:460) om etikprövning av forskning som avser människor. I tredje och fjärde stycket bemyndigas regeringen eller den myndighet som regeringen bestämmer att meddela dels föreskrifter, dels beslut i enskilda fall om undantag från förbudet i första stycket. Datainspektionen har meddelat föreskrifter som medger enskilda att i vissa fall behandla personuppgifter om lagöverträdelser m.m. (DIFS 2010:1). Som exempel kan nämnas att behandling är nödvändig för att fullgöra en föreskrift på socialtjänstområdet, för att föra anteckningar i fristående skolors elevvårdande verksamhet och för att kontrollera jävssituationer i advokatverksamhet.

Förslaget till uppgiftsskyddsförordning

Enligt artikel 9.1 i Kommissionens förslag till uppgiftsskyddsförordning är det förbjudet att behandla personuppgifter om fällande domar i brottmål eller därmed sammanhängande säkerhetsåtgärder.

I 9.2 j anges att förbudet i punkt 1 inte ska gälla om behandlingen utförs antingen under kontroll av en officiell myndighet eller behandlingen är nödvändig för att fullgöra en förpliktelse i lagstiftning eller bestämmelser som den registeransvarige omfattas av, eller för att genomföra en arbetsuppgift som utförs för viktiga ändamål av allmänt intresse, i den mån som den bemyndigas av unionslagstiftningen eller en medlemsstats lagstiftning som föreskriver lämpliga skyddsåtgärder. Ett fullständigt register över brottmålsdomar ska föras endast under kontroll av en myndighet.

Av artikel 9.3 följer att kommissionen ska ha befogenhet att anta delegerade rättsakter i syfte att precisera kriterierna, villkoren och de lämpliga skyddsåtgärderna för behandlingen av även denna kategori av uppgifter och de undantag som fastställs i punkt 2.

I Europaparlamentets resolution med ändringsförslag föreslås att förbudet i artikel 9.1 också ska ta sikte på administrativa åtgärder, domar, brott eller misstänkta brott. Det föreslår också att det i artikel 9.2 anges att alla register över brottmålsdomar ska föras endast under kontroll av en myndighet.

Våra överväganden

Bedömning: Det behövs ingen bestämmelse som generellt tillåter myndigheter att behandla personuppgifter om lagöverträdelser m.m. eftersom detta redan följer av dataskyddsdirektivets och personuppgiftslagens bestämmelser. Det finns inte heller något behov av att, utöver vad som redan följer av de grundläggande kraven i 9 § PuL, generellt begränsa myndigheters möjlighet att behandla denna kategori av personuppgifter.

Gällande rätt uppställer inget krav på särskilt författningsstöd för myndigheters behandling av personuppgifter om lagöverträdelser m.m.

Dataskyddsdirektivets förbud mot att behandla personuppgifter om lagöverträdelser m.m. och personuppgiftslagens motsvarande bestämmelse i 21 § riktar sig till andra än myndigheter.

För myndigheter gäller således enligt direktivet och personuppgiftslagen inga särskilda krav för att de ska få behandla denna kategori av personuppgifter. Myndigheter har således möjlighet att behandla sådana uppgifter under samma förutsättningar som gäller för övriga personuppgifter, dvs. att det är fråga om en tillåten behandling enligt 9 och 10 §§ PuL.

Det är emellertid vanligt att man i registerförfattningar reglerar i vilken utsträckning personuppgifter om lagöverträdelser m.m. får behandlas. Som exempel kan nämnas lagen (2001:181) om behandling av uppgifter i Skatteverkets beskattningsverksamhet där det i 1 kap. 7 § och 2 kap. 4 § föreskrivs att personuppgifter om lagöverträdelser m.m. och känsliga personuppgifter får behandlas under samma förutsättningar i beskattningsdatabasen och i annat sammanhang. I förarbetena till dessa bestämmelser nämns inte personuppgifter om lagöverträdelser särskilt, utan de omtalas som ”känsliga personuppgifter m.m.” (prop. 2000/01:33 s. 100 f.). Motiven för att särreglera dessa kategorier av personuppgifter förefaller alltså vara desamma. En särreglering av känsliga personuppgifter är emellertid nödvändig för att det ska vara tillåtet för t.ex. Skatteverket att behandla den typen av uppgifter, medan detta alltså inte är fallet när det gäller uppgifter om lagöverträdelser m.m. Av förarbetena framgår inte vad särregleringen i fråga om den senare kategorin av uppgifter avses tillföra i förhållande till vad som annars gäller enligt

personuppgiftslagen, exempelvis att regleringen skulle syfta till att begränsa den behandling som annars skulle vara tillåten.

Det saknas behov av att införa en särskild reglering för myndigheters behandling av personuppgifter om lagöverträdelser m.m.

Det finns alltså varken i dataskyddsdirektivet eller i personuppgiftslagen något förbud för myndigheter att behandla personuppgifter om lagöverträdelser m.m. Det ställs således inget krav på att det införs särskilda regler för att det ska vara tillåtet för myndigheter att behandla denna kategori av uppgifter. Någon generell bestämmelse som tillåter myndigheter att behandla personuppgifter om lagöverträdelser m.m. behövs alltså inte. Vi föreslår därför inte någon sådan bestämmelse.

Frågan blir därefter om det finns ett generellt behov av att begränsa myndigheters möjlighet att behandla denna kategori av personuppgifter i likhet med vad som ibland förekommer i registerförfattningar. Ett sådant behov skulle kunna föreligga om det finns en särskild anledning att anta att de grundläggande kraven i 9 § PuL inte utgör ett tillräckligt ”skydd” för denna kategori av uppgifter.

I likhet med vad som gäller i fråga om känsliga personuppgifter kan uppgifter om lagöverträdelser m.m. komma in till myndigheten genom en inlaga från en person som har ett ärende aktuellt hos myndigheten, oavsett om myndigheten har bett om det eller inte. Det finns således ett generellt behov hos myndigheterna av att kunna behandla även denna kategori av uppgifter inom ramen för sina sedvanliga förvaltningsuppgifter. Till skillnad från vad som gäller i fråga om känsliga personuppgifter torde det däremot vara en relativt begränsad grupp myndigheter som har behov av att för egen del samla in och behandla personuppgifter om lagöverträdelser m.m. Om så är fallet, beror det på att myndigheten har fått i uppdrag att bedriva en verksamhet där denna typ av uppgifter behövs. Redan därigenom bör det således vara tydligt vilka myndigheter som behöver behandla denna typ av uppgifter för att kunna utföra sina uppgifter. För dessa myndigheter bör det således redan vara särskilt uttryckt eller stå klart på annat sätt för vilka konkreta ändamål och på vilket sätt personuppgifter om lagöverträdelser m.m. får behandlas. Myndigheter som inte behöver behandla denna kategori av uppgifter för att kunna utföra sina uppgifter torde följakt-

ligen inte heller kunna formulera något ändamål som kan motivera en sådan behandling. Enligt vår uppfattning innebär de grundläggande kraven i 9 § således en tillräcklig begränsning för myndigheters möjlighet att behandla personuppgifter om lagöverträdelser m.m., liksom beträffande övriga personuppgifter. Vi föreslår därför inte att det införs någon generell begränsning i fråga om myndigheters möjlighet att behandla denna kategori av personuppgifter.

9.3.3 Personnummer och samordningsnummer

Allmänna dataskyddsrättsliga regler

Dataskyddsdirektivet

Enligt artikel 8.7 ska medlemsstaterna bestämma på vilka villkor ett nationellt identifikationsnummer eller något annat vedertaget sätt för identifiering får behandlas.

Personuppgiftslagen

Enligt 22 § PuL får uppgifter om personnummer eller samordningsnummer behandlas utan samtycke bara när det är klart motiverat med hänsyn till

a) ändamålen med behandlingen,

b) vikten av en säker identifiering, eller

c) något annat beaktansvärt skäl.

Av förbetena till 22 § PuL framgår att bestämmelserna i princip oförändrade i sak har överförts från den tidigare datalagen (1973:289). Regeringen anförde i sammanhanget att om någon ger sitt samtycke är det självklart att personnummer också ska få behandlas (prop. 1997/98:44 s. 77). Vidare påpekades, med anledning av att datalagens bestämmelse om återgivande av personnummer på datautskrifter inte hade överförts till nya lagen, att redan den överförda huvudregeln innebär att en uppgift om personnummer får behandlas bara när den behandlingen är klart motiverad med hänsyn till något beaktansvärt skäl. Att ha en särskild regel med annat rekvisit

– särskilda skäl – om just den behandling som själva återgivandet utgör skulle enligt regeringen bara grumla regleringen.

Av 50 § c PuL följer att regeringen eller den myndighet som regeringen bestämmer kan meddela närmare föreskrifter om i vilka fall användning av personnummer är tillåten.

Bemyndigandet har utnyttjats av regeringen bl.a. på så sätt att det i 12 § tredje stycket PuF föreskrivs att en kommun, ett landsting eller ett kommunalförbund aldrig får föra över personnummer eller samordningsnummer till tredjeland.

Förslaget till uppgiftsskyddsförordning

Kommissionens förslag till uppgiftsskyddsförordning innehåller inte någon motsvarande bestämmelse som den i dataskyddsdirektivet. Den uppställer alltså inget krav på medlemsstaterna att bestämma på vilka villkor ett nationellt identifikationsnummer m.m. får behandlas.

Våra överväganden och förslag

Förslag och bedömning: Bestämmelsen i 22 § PuL bör inte gälla för myndigheter utan 9 § innebär tillräckliga krav för när behandling av personnummer eller samordningsnummer är tillåten. Däremot bör det införas en ny bestämmelse som innebär att denna kategori av uppgifter får tas in i ett beslut endast om beslutet rör frågan om någons identitet eller motsvarande personliga förhållanden, det är nödvändigt för att beslutet ska kunna verkställas eller om det krävs med hänsyn till beslutande myndighets behov av identifieringsuppgifter.

Regeringen eller den myndighet som regeringen bestämmer bör också i fortsättningen ha möjlighet att meddela bestämmelser om i vilka fall behandling av personnummer och samordningsnummer är tillåten.

Vad innebär gällande rätt i fråga om myndigheters möjlighet att behandla uppgifter om personnummer och samordningsnummer?

Det kan konstateras att dataskyddsdirektivet ställer upp ett krav på att medlemsstaterna ska bestämma på vilka villkor som ett nationellt identifikationsbegrepp får behandlas. Direktivet föreskriver dock inte hur dessa villkor ska se ut. Det står alltså medlemsstaterna fritt att bestämma detta.

Enligt 22 § PuL gäller att myndigheter får behandla uppgifter om personnummer och samordningsnummer under samma förutsättningar som gäller för enskilda. Sådan behandling får utan samtycke ske bara när det är klart motiverat med hänsyn till ändamålen med behandlingen (a), vikten av en säker identifiering (b) eller något annat beaktansvärt skäl (c).

I registerförfattningar hänvisas ofta till att 22 § PuL gäller även vid en behandling enligt den författningen. Om en registerförfattning innehåller särskilda bestämmelser som tar sikte på behandling av personuppgifter i en databas, ingår ofta personnummer i den uppräkning av personuppgifter som får behandlas i databasen med hänvisning till de ändamål för vilka behandling av personuppgifter får ske. Som exempel på sådan reglering kan nämnas registerförfattningarna på skatte- respektive socialförsäkringsområdet (1 kap. 3 § andra stycket och 2 kap. 3 § lagen [2001:181] om behandling av uppgifter i Skatteverkets beskattningsverksamhet samt 114 kap. 15 § första stycket SFB). Genom särregleringen har det således gjort klart att behandling av personnummer och samordningsnummer i databasen är klart motiverad om den sker för de ändamål som gäller för behandling av personuppgifter i den aktuella verksamheten.

Bestämmelserna i 22 § PuL om när personnummer får användas har alltså överförts från den tidigare datalagen. Motsvarande bestämmelser fanns i 7 § andra stycket datalagen. Den paragrafens första stycke föreskrev de allmänna villkoren för att ett personregister skulle få inrättas och hur det skulle föras. I fråga om registrering av personnummer gällde dessutom att registrering fick ske endast när det var klart motiverat med hänsyn till registrets ändamål, vikten av en säker identifiering eller av annat beaktansvärt skäl. Vidare gällde att personnummer fick återges på datautskrifter endast när det

fanns särskilda skäl. Denna sista mening överfördes inte till personuppgiftslagen eftersom den ansågs obehövlig.

I förarbetena till 7 § andra stycket datalagen (prop. 1990/91:60 s. 69) anfördes bl.a. följande. Användningen av personnummer i registersammanhang bör alltid prövas från integritetssynpunkt, och onödig användning ska betraktas som integritetsintrång. Registreringen ska vara påkallad av något skäl. Det ska vara fråga om ett skäl som objektivt framstår som befogat. Fall då det kan finnas sådana objektiva skäl är bl.a. vissa forskningsregister och andra register där det är särskilt viktigt med en säker identifiering, t.ex. för att tillgodose förutsedda framtida forskningsbehov.

Av 7 § andra stycket datalagen framgick att en registrering av personnummer var tillåten om det var klart motiverat antingen med hänsyn till registrets ändamål eller på grund av vikten av en säker identifiering eller av annat beaktansvärt skäl. Om ändamålet med registret i sig inte motiverade att personnummer registrerades kunde alltså en registrering ändå vara tillåten, om den var klart motiverad med hänsyn till vikten av en säker identifiering eller något annat beaktansvärt skäl.

Formuleringen i 7 § andra stycket datalagen överfördes till 22 § PuL i princip oförändrad med undantag för att ordet register byttes ut mot ordet behandling. Det innebär att bestämmelsen i personuppgiftslagen har fått ett betydligt vidare tillämpningsområde än bestämmelsen i datalagen, som bara omfattade användning av personnummer i personregister. Den ska nu tillämpas vid all behandling av personnummer och samordningsnummer (Öman/Lindblom, s. 348). En konsekvens av att bestämmelsen nu riktar sig mot all behandling av sådana uppgifter, och inte bara i personregister, är att vad som sägs i 22 § a PuL även torde innefatta det som föreskrivs i b och c. Att personnummer och samordningsnummer kan få behandlas om det är klart motiverat med hänsyn till vikten av en säker identifiering eller något annat beaktansvärt skäl har således inte längre någon självständig betydelse, utan får uppfattas som en exemplifiering av vad som kan vara ett godtagbart ändamål.

Enligt 9 § första stycket f PuL får inte fler uppgifter behandlas än vad som är nödvändigt med hänsyn till ändamålet, vilket också kan uttryckas som att det ska vara klart motiverat att en uppgift om personnummer behandlas. Vidare sägs i samma stycke c att personuppgifter bara får samlas in för särskilda, uttryckligt angivna och

berättigade ändamål. Berättigade ändamål torde innebära detsamma som beaktansvärda skäl. I 22 § nämns dock uttryckligen att vikten av en säker identifiering är ett beaktansvärt skäl som kan motivera att uppgifter om personnummer eller samordningsnummer får behandlas. Det utgör alltså en komplettering i förhållande till de krav som annars redan gäller enligt 9 § PuL.

Eftersom det är fråga om att använda personuppgifter som utgör hjälpmedel för identifikation, kan man fråga sig om inte vikten av en säker identifiering är ett så självklart godtagbart ändamål att det inte behöver nämnas särskilt i lagtexten. Att det nämndes uttryckligen i 7 § datalagen hade däremot en särskild betydelse, eftersom det markerade att detta ändamål kunde utgöra ett självständigt och beaktansvärt skäl att registrera personnummer även om ändamålet med registret i sig inte kunde motivera detta.

Mot bakgrund av ovanstående kan det alltså sättas ifråga om bestämmelserna i 22 § PuL egentligen har någon självständig betydelse vid sidan av vad som redan gäller enligt de grundläggande kraven i 9 §.

Finns det behov av en särskild bestämmelse på myndighetsområdet?

Det kan alltså konstateras att innebörden av 22 § PuL är oklar både vad avser hur de uppräknande fallen i a–c förhåller sig till varandra och i vilken utsträckning bestämmelserna i sak innebär några andra krav än de som redan följer av 9 §.

På myndighetsområdet används personnummer och samordningsnummer i mycket stor utsträckning. Om personuppgifter används i en myndighets verksamhet förekommer i princip alltid också uppgifter för att fastställa den enskildes identitet, dvs. personnummer eller samordningsnummer. Det är därför inte tillfredsställande att den bestämmelse som ska tillämpas vid användning av denna typ av uppgifter inte är klar till sin innebörd. Enligt vår uppfattning bör 22 § PuL därför inte gälla på myndighetsområdet, utan vilka grundläggande krav som ska vara uppfyllda för att ett personnummer eller samordningsnummer ska få behandlas bör i stället framgå, liksom för övriga personuppgifter, av 9 §. Att vikten av en säker identifiering kan utgöra ett berättigat ändamål får i det sammanhanget anses självklart.

Vad som däremot kan vara motiverat att införa i en samlad reglering för myndigheternas behandling av personuppgifter är en bestämmelse som syftar till att utgöra ett särskilt skydd vid spridning av personnummer eller samordningsnummer. Det kan konstateras att sekretessbestämmelser som syftar till att skydda uppgifter om enskildas personliga eller ekonomiska förhållanden ofta inte gäller för en myndighets eller domstols beslut. Den möjlighet som finns att skydda personnummer eller samordningsnummer inom ramen för den verksamhet som myndigheten bedriver, vilken innebär att uppgifter i handlingar från verksamheten kan skyddas med hänsyn till sekretess, finns alltså vanligen inte när det gäller myndigheters eller domstolars avgöranden.

Bestämmelsen i 7 § andra stycket andra meningen datalagen med särskilda regler om återgivande av personnummer i datautskrifter syftade till att utgöra ett särskilt skydd i samband med spridning av personnummer. I förarbetena (prop. 1990/91:60 s. 69) anfördes att särskilda skäl för att tillåta spridning av personnummer på detta sätt kan vara att en viss mottagare behöver uppgifterna för identitetskontroll, registersökning eller registrering. Det var enligt föredragande statsrådet helt klart att mantalsskrivningsbevis, personbevis och liknande intyg fick innehålla personnummer även i fortsättningen. Mottagaren använder normalt dessa intyg för sådana ändamål att kravet på särskilda skäl är uppfyllt.

Från praxis rörande tillämpningen av 7 § andra stycket andra meningen datalagen kan nämnas regeringens beslut 1994-12-01 (Dnr Ju 94/1) om att Riksförsäkringsverket inte fick ange personnummer på utskrifter från assistansersättningsregistret. Utskrifterna skulle användas för utbetalning av ersättning. Ett annat exempel är regeringens beslut 1996-04-25 (Dnr Ju 95/2469) om att universitet och högskolor inte fick använda personnummer på tentamenslistor och liknande utskrifter som ska anslås. En utförlig redovisning av praxis rörande tillämpning av 7 § andra stycket datalagen finns i Öman/Lindblom, s. 356 f.

I samband med att 22 § PuL infördes bedömdes det inte finnas något behov av att låta bestämmelsen i 7 § andra stycket andra meningen datalagen med särskilda regler om återgivande av personnummer i datautskrifter få någon motsvarighet i personuppgiftslagen. Detta innebar enligt regeringen inte någon ändring i sak (prop. 1997/98:44 s. 77).

Det kan konstateras att ett personnummer eller samordningsnummer i sig inte kan anses integritetskränkande. Däremot kan denna kategori av uppgifter användas på ett sätt som innebär risker för den enskildes integritet. Senare tids debatt kring bedrägerier genom s.k. identitetsstöld är ett exempel på detta. En särskild risk i det sammanhanget är när denna typ av uppgifter öppet exponeras och blir föremål för spridning utan att det kan anses motiverat. En behandling av personnummer eller samordningsnummer kan alltså vara klart motiverad med hänsyn till den personuppgiftsansvariges ändamål med att behandla uppgifterna, medan det däremot inte alls är motiverat att uppgifterna sprids utanför verksamheten. De grundläggande kraven i 9 § PuL, liksom de nuvarande bestämmelserna i 22 §, innebär visserligen att personnummer eller samordningsnummer inte får behandlas genom att återges i ett beslut och därigenom öppet exponeras och spridas, om det inte är nödvändigt med hänsyn till ändamålet med att göra uppgifterna i beslutet offentliga. Denna typ av uppgifter återges emellertid i dag i myndigheters och domstolars beslut i en utsträckning som i varje enskilt fall knappast kan anses vara motiverad. Enligt vår uppfattning finns det därför skäl för att införa en bestämmelse som särskilt skyddar personnummer eller samordningsnummer i samband med upprättandet av beslut. Bestämmelsen bör inte utformas så att den hindrar spridning av avgöranden på grund av att de innehåller uppgifter om personnummer eller samordningsnummer. I stället bör skyddet för en onödig spridning åstadkommas genom en reglering som innebär en begränsning i myndigheternas möjlighet att återge personnummer eller samordningsnummer i sina avgöranden i förhållande till de grundläggande kraven i 9 § PuL, dvs. det ska gälla särskilda restriktioner även om behandlingen som sådan är tillåten. En sådan bestämmelse knyter an till den bestämmelse som tidigare fanns i 7 § andra stycket andra meningen datalagen. Därmed åstadkommer man, i likhet med syftet med den bestämmelsen, ett särskilt skydd i samband med öppen exponering av personnummer och samordningsnummer genom myndigheters och domstolars avgöranden.

Vi föreslår därför att det införs en bestämmelse som innebär att det i myndigheters avgöranden får tas in personnummer eller samordningsnummer endast när det är nödvändigt med hänsyn till vissa skäl som uttryckligen framgår av bestämmelsen. En sådan

bestämmelse förhindrar därigenom ett slentrianmässigt eller inte tillräckligt övervägt återgivande av sådana uppgifter. Samtidigt måste bestämmelsen fånga upp de skäl som kan anses motivera att denna typ av uppgifter tas in i myndighetens avgörande i en viss fråga.

Den fråga som har avgjorts genom myndighetens eller domstolens beslut kan vara av sådant slag att det är av särskild vikt att partens identitet så långt det är möjligt klargörs i avgörandet. Så kan självklart vara fallet när avgörandet i vidare mening rör frågor om parts identitet eller status, såsom t.ex. beslut rörande folkbokföring eller uppehållstillstånd. Särskilda skäl kan också finnas när det i avgörandet behandlas frågor om lagöverträdelser eller tvångsåtgärder av olika slag, då det inte får uppstå någon risk för förväxling av vilken person som berörs av avgörandet i fråga. Detsamma kan sägas om ett avgörande som i sig utgör en exekutionstitel (jfr 3 kap. 1 § utsökningsbalken) eller som t.ex. utgör ett individuellt tillstånd till något. Det förekommer vidare att det i en myndighets eller domstols avgörande anges personnummer, men inte övriga uppgifter som återger personens namn och adress. Det är då fråga om en person som har skyddade personuppgifter enligt 22 kap. 1 § OSL, s.k. folkbokföringssekretess. I de nu nämna fallen är det således frågan om situationer då personnummer eller samordningsnummer behöver återges för att beslutet ska kunna verkställas. Det finns också myndigheter vars verksamhet är uppbyggd kring användning av personnummer och där t.ex. domstolsavgörandena därför måste innehålla personnummer för att kunna knytas till rätt ärende. I sådana fall handlar det alltså om att det är nödvändigt att återge denna typ av uppgifter i beslutet för ett behov som är hänförligt till den beslutande myndigheten. Även i sådana fall kan det finnas tillräckliga skäl för att personnummer eller samordningsnummer kan tas in i beslutet.

Däremot torde det inte kunna hävdas att tredje man kan ha ett sådant behov av att känna till en parts personnummer eller samordningsnummer, utöver de situationer då sådana uppgifter behövs för att kunna verkställa beslutet, att det särskilt kan motivera att sådana uppgifter återges i ett myndighetsbeslut.

Vi föreslår därför att personnummer eller samordningsnummer får återges i en myndighets beslut endast om beslutet i vidare mening rör frågan om någons identitet eller det är nödvändigt för

att beslutet ska kunna verkställas eller om det krävs med hänsyn till den beslutande myndighetens behov av identifieringsuppgifter.

Bemyndiganden att meddela ytterligare föreskrifter

Det kan också i fortsättningen finnas behov av att på vissa myndighetsområden införa särskilda bestämmelser om när behandling av personnummer och samordningsnummer är tillåten. Regeringen eller den myndighet som regeringen bestämmer bör därför, i likhet med vad som i dag gäller enligt 50 § c PuL, ha möjlighet att meddela närmare bestämmelser om i vilka fall behandling av personnummer och samordningsnummer är tillåten.

9.4 Sökbegränsningar

9.4.1 Allmänna utgångspunkter

I myndigheternas verksamhet finns ett behov av att kunna använda sig av den information som myndigheten har tillgång på ett så effektivt sätt som möjligt. Att information numera i princip undantagslöst hanteras elektroniskt inom myndigheterna innebär dels bättre möjligheter och enklare förfaranden för att över huvud taget producera information i form av bl.a. olika dokument och uppgiftssamlingar, dels väsentligt förbättrade möjligheter att sammanställa den information som myndigheten har tillgång till. Den elektroniskt framställda informationen utgör därigenom ett kraftfullt verktyg för att uppnå effektivitet och utgör således ett värdefullt hjälpmedel för att uppnå hög kvalitet i exempelvis beslutsunderlag, vid uppföljning och när det gäller att uppfylla skyldigheter och ge service i förhållande till parter och andra enskilda.

Möjligheten att kunna söka och sammanställa information är således mycket värdefull för myndigheterna och något som de allmänt får anses ha ett stort behov av. Samtidigt som möjligheten att elektroniskt kunna sammanställa information är ett kraftfullt verktyg för att uppnå en effektiv informationshantering, kan den emellertid innebära särskilda risker för skyddet av personuppgifter. Redan på datalagens tid fanns därför bestämmelser om att Datainspektionen i sina tillstånd för att inrätta och föra ett person-

register skulle meddela föreskrifter om de bearbetningar av personuppgifterna i registret som fick göras med automatisk databehandling, om det behövdes för att förebygga risk för otillbörliga intrång i den enskildes personliga integritet (6 § första stycket 5). Det förekom alltså redan före personuppgiftslagens införande föreskrifter i fråga om begränsningar i möjligheterna att söka fram och sammanställa personuppgifter dels i beslut av Datainspektionen, dels genom bestämmelser i den tidens registerförfattningar.

Dataskyddsdirektivet och personuppgiftslagen innehåller inte några bestämmelser som särskilt tar sikte på att skydda personuppgifter i samband med sammanställning av uppgifter. Sökning och sammanställning av uppgifter som sker elektroniskt är emellertid en form av behandling som omfattas av direktivets och personuppgiftslagens bestämmelser om det är fråga om personuppgifter.

Av de grundläggande kraven i 9 § PuL följer emellertid vissa begränsningar i fråga om vilka sammanställningar som är tillåtna att göra. Som exempel kan nämnas att en sammanställning av personuppgifter inte får göras för ett ändamål som är oförenligt med det för vilket uppgifterna en gång samlades in, att uppgifterna ska vara adekvata och relevanta för ändamålet med sammanställningen och att inte fler uppgifter än vad som är nödvändigt för ändamålet med behandlingen får sammanställas.

I många registerförfattningar finns bestämmelser som uttryckligen reglerar vilka sökbegrepp som alltid är förbjudna att använda och som således omöjliggör en sammanställning utifrån dessa personuppgifter. Man kan säga att sådana begränsningar utgör en miniminivå för det skydd som vid en tillämpning av 9 § PuL ändå ska iakttas av myndigheten när den söker och sammanställer personuppgifter. Den typen av förbud utgör också ett hinder för en myndighet att sammanställa personuppgifter på begäran av en enskild i enlighet med den s.k. begränsningsregeln i 2 kap. 3 § tredje stycket TF. Sådana sökbegränsningar utgör således ett absolut hinder för en myndighet när det gäller dess möjlighet att sammanställa uppgifter för behov både i den egna verksamheten och i fråga om en begäran från en enskild inom ramen för dennes rätt att ta del av allmänna handlingar enligt bestämmelserna i 2 kap. TF. Det finns därför anledning att överväga om det i den nya lagen bör finnas sådana sökbegränsningar som ska gälla generellt.

9.4.2 Våra överväganden och förslag

Förslag och bedömning: Det införs en bestämmelse som innebär att myndigheter vid en sökning får som sökbegrepp använda uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening eller uppgifter som rör hälsa eller sexualliv endast i den utsträckning som det finns särskilt författningsstöd för det. Sådant stöd kan anges genom föreskrifter som tas in i bilagan till lagen, i annan lag eller i förordning. Därmed gäller alltså som huvudregel ett generellt förbud för myndigheter att som sökbegrepp använda uppgifter som leder till att känsliga personuppgifter sammanställs.

I bestämmelsen bör klargöras att detta förbud inte gäller vid sökning i en viss handling eller i ett visst ärende.

Något behov av att generellt förbjuda myndigheter att använda andra kategorier av personuppgifter som sökbegrepp finns inte. I lagen tas in ett bemyndigande som tillåter regeringen att meddela sådana föreskrifter i de fall det finns ett särskilt behov av detta.

Sökbegränsningar i fråga om känsliga personuppgifter

Vi har i avsnitt 9.3 konstaterar att alla myndigheter kan ha ett behov av att behandla känsliga personuppgifter. Det beror på att en myndighet till viss del inte kan kontrollera huruvida den typen av uppgifter förekommer i dess informationssamlingar eftersom exempelvis parter i en myndighets ärenden själva kan uppge sådana uppgifter i t.ex. en inlaga till myndigheten. Enligt vårt förslag ska det, såsom undantag från det principiella förbudet i 13 § PuL, vara tillåtet för myndigheter att behandla känsliga personuppgifter både i löpande text och inom ramen för ett ärendehanteringssystem. Det sistnämnda innebär att känsliga personuppgifter kan förekomma i större informationssamlingar, där storleken bestämts utifrån hur myndigheten väljer att koppla ihop olika ärenden med varandra. Inom en sådan informationssamling kan det alltså vara tekniskt möjligt att söka och sammanställa även känsliga personuppgifter.

Många registerförfattningar innehåller sökbegränsningar som tar sikte på känsliga personuppgifter. Det brukar ibland uttryckas så att det är en känslig personuppgift som inte får användas som sökbegrepp (se t.ex. prop. 2009/10:85 s. 155). Personuppgifter är i dataskyddsdirektivets mening all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet (artikel 2). Det är alltså frågan om uppgifter som kan knytas till en viss person. En personuppgift är känslig om den exempelvis rör hälsa. Det ska således vara frågan om en uppgift som rör en viss persons hälsa. Ordet ”schizofren” är en uppgift som används för att beteckna ett visst hälsotillstånd hos de personer som lider av detta. Det kan därför i någon mening anses vara en personuppgift. Det är emellertid inte en personuppgift i direktivets mening, eftersom ordet i sig inte tar sikte på en viss person. Om det i en författning har föreskrivits att känsliga personuppgifter inte får användas som sökbegrepp kan man därför få intrycket av att vad som avses är att det i fråga om en viss person inte får göras en sökning som förknippar denne med en uppgift som rör hans eller hennes hälsa. Vad som åsyftas är emellertid att det inte ska vara tillåtet att göra en sammanställning som innehåller personuppgifter genom att t.ex. använda ordet ”schizofren” som sökbegrepp, dvs. ett ord som i sig inte är en personuppgift men som rör hälsa. Resultatet av en sådan sökning kommer då att utgöra en sammanställning av de personer som förekommer i den aktuella informationssamlingen till vilka detta ord kan hänföras. Genom att använda ett visst ord som sökbegrepp, som i sig inte är en personuppgift, i syfte att göra en sammanställning som innehåller personuppgifter kan således känsliga personuppgifter avslöjas. En motsvarande sökning i syfte att göra en sammanställning som inte innehåller personuppgifter i direktivets mening, exempelvis i en databas för vetenskaplig referenslitteratur, omfattas däremot inte av en sådan sökbegränsning.

Det torde enligt vår mening bara vara ett begränsat antal myndigheter som för den egna verksamheten kan sägas ha något egentligt behov av att kunna göra sammanställningar av känsliga personuppgifter inom ramen för sina ärendehanteringssystem eller andra informationssamlingar som hos myndigheten innehåller personuppgifter. Det talar för att det kan finnas skäl att i den nya lagen införa en generell begränsning som tar sikte på möjligheterna att göra sammanställningar i den information som samlats hos myndig-

heterna såvitt avser känsliga personuppgifter. Många registerförfattningar innehåller, som redan påpekats, sådana sökbegränsningar. Enligt vår uppfattning finns det därför ett behov av att i den nya lagen ha en bestämmelse som innebär en sådan begränsning. Vid en sökning bör det därför vara tillåtet att som sökbegrepp använda uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening eller uppgifter som rör hälsa eller sexualliv endast i den utsträckning som det finns särskilt författningsstöd för det. Sådant stöd kan ges genom föreskrifter som tas in i bilagan till lagen, i annan lag eller i förordning. Enligt lagen kommer därmed som huvudregel att gälla ett generellt förbud för myndigheter att som sökbegrepp använda uppgifter som leder till att känsliga personuppgifter sammanställs. Vi föreslår alltså att det införs en bestämmelse med detta innehåll.

Förbudet mot att använda sådana uppgifter som sökbegrepp som leder till att känsliga personuppgifter sammanställs ska inte gälla vid sökning i en viss handling eller i ett visst ärende. Det bör framgå uttryckligen av den bestämmelse som vi nu föreslår.

Sökbegränsningar i fråga om andra särskilda kategorier av personuppgifter

Uppgifter om lagöverträdelser m.m.

I avsnitt 9.3 har vi vidare gjort bedömningen att det inte behöver införas några särskilda regler vare sig när det gäller att tillåta myndigheter att behandla personuppgifter om lagöverträdelser m.m. eller att begränsa användandet av den typen av uppgifter utöver vad som redan följer av de grundläggande kraven i 9 § PuL.

Skälet till att vi bedömer att det inte genom en särskild bestämmelse behöver införas en begränsning när det gäller en myndighets behandling av personuppgifter om lagöverträdelser m.m. är bl.a. att myndigheter, till skillnad från vad som är fallet med känsliga personuppgifter, endast i begränsad utsträckning för egen del kan behöva samla in och behandla den typen av uppgifter. Den typen av uppgifter kan därför inte sägas generellt sett vara vanligt förekommande i myndigheters informationssamlingar. Till skillnad från vad som är fallet med känsliga personuppgifter, som kan före-

komma i stort sett hos vilken myndighet som helst, är situationen vad beträffar uppgifter om lagöverträdelser m.m. alltså inte sådan att det på grund av innehållet i myndigheternas informationssamlingar allmänt sett finns ett behov av att uppväga den risk som uppstår för enskildas integritetsskydd genom särskilda bestämmelser om sökbegränsningar. Det torde därför inte finnas något behov av att införa ett generellt sökförbud – som då skulle behöva förses med en hel rad undantag – när det gäller den typen av uppgifter för att begränsa myndigheters möjligheter att göra sammanställningar av sådana uppgifter.

Som redan påpekats syftar ett sökförbud också till att utgöra ett särskilt skydd för den aktuella kategorin personuppgifter i samband med att myndigheten fullgör sin skyldighet enligt 2 kap. 3 § TF att sammanställa uppgifter på begäran av en enskild. Om ett förbud att använda uppgifter om lagöverträdelser m.m. inte införs innebär det således att en myndighet i princip är skyldig att göra en sammanställning av sådana uppgifter om en sådan begärs ut, så länge den kan göras med rutinbetonade åtgärder. Det förutsätter emellertid att uppgifterna inte skyddas av sekretess.

För den händelse det är fråga om ett myndighetsområde där ett omvänt skaderekvisit gäller för uppgifter om enskilds personliga förhållanden, dvs. en presumtion för sekretess, torde det finnas små möjligheter att lämna ut uppgifter om lagöverträdelser m.m. Ett svagare sekretesskydd finns dock om sekretess gäller med ett rakt skaderekvisit, dvs. med presumtion för offentlighet. Det torde bero på sammanhanget om en uppgift om lagöverträdelser m.m. är att anse som typiskt sett känslig och därför skulle omfattas av sådan sekretess.

Enligt 21 § PuL är det dock som huvudregel förbjudet för andra än myndigheter att behandla uppgifter om lagöverträdelser m.m. Det innebär att en begäran från en enskild om att från en myndighet få ut en sammanställning av personuppgifter om lagöverträdelser m.m. torde aktualisera en prövning enligt 21 kap. 7 § OSL. Om den enskildes åsyftade behandling av uppgifterna inte tillhör de undantagsfall då en sådan behandling är tillåten för enskilda, utgör 21 kap. 7 § OSL ett hinder mot att lämna ut uppgifterna. Mot bakgrund av att det endast i undantagsfall är tillåtet för enskilda att behandla personuppgifter om lagöverträdelser m.m. utgör enligt vår uppfattning 21 kap. 7 § OSL ett tillräckligt skydd för denna typ av

uppgifter i fråga om skyldigheten att göra sammanställningar på begäran av en enskild. Vi bedömer därför att det inte heller på grund av en myndighets skyldighet enligt 2 kap. 3 § TF finns ett behov av att införa ett generellt förbud mot använda uppgifter om lagöverträdelser m.m. som sökbegrepp.

Uppgifter om personnummer och samordningsnummer

Vi har i avsnitt 9.3.3 funnit att 9 § PuL innehåller tillräckliga krav för att personuppgifter om personnummer och samordningsnummer ska ges ett tillfredsställande skydd när myndigheter behandlar denna typ av uppgifter, med undantag för när det gäller återgivande av sådana uppgifter i myndigheters beslut.

Om ett personnummer används som sökbegrepp innebär det att man, när detta är tekniskt möjligt, kan söka fram och sammanställa exempelvis alla ärenden om en viss person hos en viss myndighet. Det kan konstateras att myndigheter allmänt sett får anses ha ett stort och i hög grad berättigat behov av att kunna göra den typen av sökningar och det kan inte anses typiskt sett integritetskänsligt att så sker.

Mot den bakgrunden kan det enligt vår bedömning inte anses motiverat att införa något ytterligare sådant skydd som ett generellt sökförbud kan utgöra i samband med utlämnanden av nu aktuella personuppgifter enligt 2 kap. TF utöver det skydd som redan ges genom bestämmelser om sekretess.

Vi föreslår därför inte någon generell begränsning när det gäller myndigheters möjlighet att använda personuppgifter om personnummer och samordningsnummer som sökbegrepp.

Sökbegränsningar i fråga om övriga personuppgifter

Vi har i avsnitt 9.3 bedömt att det inte behövs några särskilda bestämmelser, utöver 9 § PuL, om vilka övriga personuppgifter som får eller inte får behandlas. I registerförfattningar förekommer i allmänhet inte bestämmelser som syftar till att begränsa användningen av personuppgifter, som inte hör till de särskilda kategorierna av uppgifter, som sökbegrepp. Däremot förekommer begränsningar som tar sikte på att söka fram enskilda handlingar i data-

baser. Det brukar då anges vilka sökbegrepp som får användas, exempelvis namn och ärendenummer.

Det finns emellertid ett undantag från det som nu sagts och det rör uppgifter som avslöjar nationell anknytning.

Vårt förslag innebär att det blir förbjudet för myndigheterna att använda uppgifter som avslöjar eller rör känsliga personuppgifter som sökbegrepp. Därigenom kan uppgifter som avslöjar ras eller etniskt ursprung inte användas som sökbegrepp. Uppgifter om en persons nationalitet har i lagstiftning som rör behandling av personuppgifter inte ansetts vara uppgifter som normalt avslöjar ras eller etniskt ursprung (prop. 2009/10:85 s. 325). I 1 kap. 5 § första stycket 2 diskrimineringslagen (2008:567) definieras emellertid begreppet etnisk tillhörighet som nationellt eller etniskt ursprung, hudfärg eller annat liknande förhållande. Av detta förhållande kan emellertid inte slutsatsen dras att uppgifter om en persons nationalitet i dataskyddsdirektivets mening alltid är att betrakta som en känslig personuppgift. En sådan uppgift blir dock känslig om den i det enskilda fallet skulle avslöja etniskt ursprung.

I flertalet fall är en uppgift om nationalitet alltså inte en uppgift som är känslig. Det kan dock finnas situationer där det finns ett behov av att skydda uppgifter som avslöjar nationalitet, exempelvis för att förhindra att personer utsätts för förföljelse. Av det skälet gäller enligt 21 kap. 5 § OSL sekretess för uppgift som rör en utlänning, om det kan antas att röjande av uppgiften skulle medföra fara för att någon utsätts för övergrepp eller lider annat allvarligt men som föranleds av förhållanden mellan utlänningen och en utländsk stat eller myndighet eller organisation av utlänningar. Sekretessen är inte begränsad till någon viss verksamhet, utan ska tillämpas hos alla myndigheter. I verksamhet för kontroll av utlänningar gäller vidare enligt 37 kap. 1 § OSL ett mer allmänt sekretesskydd för uppgift om enskilds personliga förhållanden.

I Skatteverkets folkbokföringsverksamhet förekommer uppgifter som avslöjar nationell anknytning i stor utsträckning. I 2 kap. 10 § lagen (2001:182) om behandling av personuppgifter i Skatteverkets folkbokföringsverksamhet finns förbud mot att använda vissa uppgifter som avslöjar nationell anknytning. Exempelvis gäller att uppgifter om medborgarskap får användas endast i fråga om medborgarskap i Sverige, Danmark, Norge, Finland och Island samt om

medborgarskap inom eller utom EU (unionsmedborgarskap eller icke unionsmedborgarskap).

Även i de förordningar som för närvarande reglerar behandling av personuppgifter hos domstolarna finns bestämmelser som förbjuder domstolarna att använda uppgifter om nationalitet som sökbegrepp. I förslaget till en ny domstolsdatalag föreslås också sådana begränsningar.

Det kan alltså konstateras att en uppgift om en persons nationalitet kan vara en känslig personuppgift i dataskyddsdirektivets mening om den avslöjar personens etniska ursprung. Så är emellertid normalt inte fallet. Enligt vår uppfattning finns det därför inget behov av att införa bestämmelser i den nya lagen som generellt begränsar myndigheters möjlighet att använda uppgifter om nationalitet som sökbegrepp för behov som kan finnas för att den egna verksamheten ska kunna utföras. I den mån det i viss myndighetsverksamhet finns ett särskilt behov av begränsningar, exempelvis för att det där förekommer uppgifter om nationalitet i stor utsträckning som i Skatteverkets folkbokföringsverksamhet eller hos domstolarna, finns det inget som hindrar att det införs sådana bestämmelser.

Det kan vidare konstateras att det vid utlämnanden från alla myndigheter finns möjlighet att med hänsyn till behovet av att skydda någon från förföljelse hindra utlämnande av uppgifter om nationalitet genom sekretessbestämmelsen i 21 kap. 5 § OSL.

Behov av andra begränsningar i särskilda fall

Om det finns ett särskilt behov av att begränsa möjligheterna till sökning och sammanställning av personuppgifter i en viss myndighetsverksamhet, exempelvis för att det i likhet med folkbokföringen är vanligt med uppgifter om nationell anknytning, innebär den generella lagen inget hinder mot att genom en bestämmelse i lag eller förordning meddela särskilda bestämmelser om sökbegränsningar. En sådan bestämmelse kommer därmed att utgöra en precisering av de grundläggande krav som gäller enligt 9 § PuL, till vilken den nya lagen hänvisar. I den mån sådana begränsningar tar sikte på en kommun, kan de anses innebära ett åliggande för kommunen. Regeringen bör därför bemyndigas i den nya lagen att meddela

föreskrifter om begränsningar i möjligheterna att använda andra sökbegrepp än sådana som avslöjar känsliga personuppgifter.

10 Personuppgiftsansvar och säkerhet

10.1 Personuppgiftsansvar

10.1.1 Allmänna dataskyddsrättsliga regler

Dataskyddsdirektivet

Utgångspunkten enligt dataskyddsdirektivet är att det alltid ska finnas någon som bär ansvaret för att dataskyddsreglerna följs vid behandling av personuppgifter och som den enskilde registrerade kan vända sig till för att göra gällande sina rättigheter. I direktivet används begreppet registeransvarig som benämning på den ansvarige (controller i direktivets engelska version). Registeransvaret är vidare en utgångspunkt när det ska bedömas vilken medlemsstats lagstiftning som är tillämplig på en viss personuppgiftsbehandling och, följaktligen, vilket lands tillsynsmyndighet som är behörig att vidta åtgärder.

Begreppet registeransvarig definieras i artikel 2 d direktivet på följande sätt.

> Registeransvarig: den fysiska eller juridiska person, den myndighet, den institution eller det andra organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter. När ändamålen och medlen för behandlingen bestäms av nationella lagar och andra författningar eller av gemenskapsrätten kan den registeransvarige eller de särskilda kriterierna för att utse honom anges i nationell rätt eller i gemenskapsrätten.

Av definitionen följer att registeransvaret kan vara gemensamt för flera personer eller organ.

Utöver begreppet registeransvarig definieras bl.a. begreppet registerförare (processor på engelska) såsom den fysiska eller juridiska

person, den myndighet, den institution eller det andra organ som behandlar personuppgifter för den registeransvariges räkning (artikel 2 f).

Dessa definitioner ger viss ledning i fråga om vilka slags organ vid sidan av fysiska personer som kan vara registeransvariga eller registerförare. Begreppet registeransvarig (respektive begreppet registerförare) tar sikte på organet som sådant och inte på någon enskild person inom organet ifråga, t.ex. någon viss personlig företrädare för organet eller någon av dem som faktiskt behandlar uppgifterna, dvs. som utgör s.k. medhjälpare och i den egenskapen behandlar personuppgifter under den registeransvariges eller registerförarens direkta ansvar.

Personuppgiftslagen

I personuppgiftslagen används begreppen personuppgiftsansvarig och personuppgiftsbiträde i stället för dataskyddsdirektivets uttryck registeransvarig respektive registerförare. Definitionerna i 3 § PuL av personuppgiftsansvarig och personuppgiftsbiträde är i sak identiska med direktivets (prop. 1997/98:44 s. 119) dock att det i definitionen av personuppgiftsansvarig inte tagits med dels det som nämns i direktivet om vad för slags aktör som kan vara ansvarig eller biträde, dels vad som gäller när ändamålen och medlen för behandlingen bestäms av nationella lagar och andra författningar eller av unionsrätten. Personuppgiftsansvarig är enligt 3 § PuL den som ensam eller tillsammans med andra bestämmer ändamålen med eller medlen för behandlingen av personuppgifter.

Förslaget till uppgiftsskyddsförordning

Definitionen av registerförare är densamma i kommissionens förslag till uppgiftsskyddsförordning som i dataskyddsdirektivet. Liksom för närvarande lämnas ett utrymme för medlemsstater att i nationell reglering fastställa vem som är personuppgiftsansvarig.

I artikel 24 finns en bestämmelse som syftar till att klargöra gemensamma registeransvarigas ansvar vad avser förhållandet dem emellan och gentemot den registrerade. Artikeln med rubriken Gemensamma registeransvariga har följande lydelse.

> Om en registeransvarig fastställer ändamålen, villkoren och medlen för behandlingen av personuppgifter tillsammans med andra ska de gemensamma registeransvariga fastställa sitt respektive ansvar för att fullgöra skyldigheterna enligt denna förordning, särskilt avseende förfarandena och rutinerna för den registrerades utövande av sina rättigheter, genom ett arrangemang som de enas om sinsemellan.

Europaparlamentet har i sin resolution med förslag till ändringar i uppgiftsskyddsförordningen föreslagit ett tillägg i artikel 24 om att arrangemanget ska återspegla de gemensamma registeransvarigas respektive roller och förhållanden gentemot den registrerade. Det väsentliga innehållet i arrangemanget ska göras tillgängligt för den registrerade. I fall av oklar ansvarsfördelning ska var och en av de registeransvariga vara solidariskt ansvariga.

Genom artikel 26 anges registerförares (dvs. personuppgiftbiträdens) ställning och skyldigheter. Bestämmelserna innebär bl.a. att en registerförare som behandlar andra personuppgifter än de som anges i den registeransvariges instruktioner ska anses som en gemensam registeransvarig. Vidare ska i avtalet mellan den registeransvarige och registerföraren föreskrivas att en registerförare får engagera en annan registerförare bara om den registeransvarige först har godkänt det, att registerföraren ska lämna alla resultat till den registeransvariga vid behandlingens slut och inte behandla personuppgifterna på annat sätt och att både den registeransvarige och tillsynsmyndigheten ska ges tillgång till all information som krävs för att kontrollera registerförarens skyldigheter enligt artikel 26. En nyhet är också att den registeransvarige och registerföraren skriftligen ska dokumentera den registeransvariges instruktioner till registerföraren.

10.1.2 Allmänt om personuppgiftsansvar och om personuppgiftsbiträden

Personuppgiftsansvaret innebär bl.a. en skyldighet att se till att de i 9 § PuL angivna grundläggande kraven på behandling av personuppgifter iakttas. Vidare innebär personuppgiftsansvaret en skyldighet att självmant och på särskild begäran lämna information till den registrerade (23–27 §§), att på den registrerades begäran rätta, blockera eller utplåna personuppgifter som inte behandlats i enlighet med personuppgiftslagen (28 §), att vidta lämpliga tekniska och

organisatoriska åtgärder för att skydda de personuppgifter som behandlas (31 §), att – enligt huvudregeln – anmäla all automatiserad behandling av personuppgifter till tillsynsmyndigheten, dvs. Datainspektionen (36 §) samt att ersätta den registrerade för den skada en lagstridig behandling av personuppgifter för med sig (48 §).

Den personuppgiftsansvarige kan anlita ett personuppgiftsbiträde för att behandla personuppgifter för den ansvariges räkning. Ett personuppgiftsbiträde ska finnas utanför den egna organisationen och kan vara en juridisk eller fysisk person som i sin tur kan ha anställda medhjälpare vilka i praktiken är de som ombesörjer personuppgiftsbehandlingen under personuppgiftsbiträdets direkta ansvar. Ett personuppgiftsbiträde och dennes medhjälpare anses inte vara tredje man i personuppgiftslagens mening (3 §). De kan därför utan hinder av de bestämmelser i personuppgiftslagen som gäller utlämnande till tredje man få del av de personuppgifter som ska behandlas för den ansvariges räkning.

Personuppgiftsbiträden kan i sin tur anlita ”underbiträden”. Datainspektionen har för situationer där ett huvudbiträde anlitar ett eller flera underbiträden ansett att kravet på personuppgiftsbiträdesavtal kan uppfyllas genom att den personuppgiftsansvarige ger ett huvudbiträde mandat att ingå avtal med underbiträden. Av ett sådant avtal måste framgå att varje underbiträde har samma skyldigheter som huvudbiträdet. Den personuppgiftsansvarige ska alltid ha kännedom om vilka personuppgiftsbiträden som behandlar personuppgifter för dennes räkning. I annat fall kan den personuppgiftsansvarige inte uppfylla säkerhetskraven och kraven på kontroll av personuppgiftsbiträden (Datainspektionens webbplats, samrådsyttrande november 2011, dnr 1421-2011).

Ett personuppgiftsbiträde (inklusive dennes eventuella medhjälpare) får behandla personuppgifter bara i enlighet med instruktioner från den personuppgiftsansvarige (30 §). Ett skriftligt avtal med detta villkor måste upprättas mellan den personuppgiftsansvarige och personuppgiftsbiträdet. Varken av lagen eller av dataskyddsdirektivet framgår hur utförliga instruktioner som den personuppgiftsansvarige måste lämna sina medhjälpare. Datalagskommittén framhöll att den personuppgiftsansvarige i princip bär ansvaret för att instruktionerna är så tydliga att otillåten behandling inte kommer att utföras (SOU 1997:39 s. 408). Dessutom måste det föreskrivas i avtalet att personuppgiftsbiträdet är skyldigt att vidta de

tekniska och organisatoriska säkerhetsåtgärder som avses i 31 § för att skydda de behandlade personuppgifterna. Det är den personuppgiftsansvarige som ansvarar för att personuppgiftsbiträdesavtal finns. Såvitt avser behandling som sker i det allmännas verksamhet har bestämmelser i författning företräde framför instruktioner (jfr 2 § och 30 § tredje stycket PuL).

Datainspektionen brukar framhålla att instruktionerna till ett personuppgiftsbiträde ska vara så tydliga att otillåten behandling inte kommer att utföras. Instruktionerna kan exempelvis gälla ändamålen med behandlingen, tredjelandsöverföring och utlämnande till tredje man. Vad gäller kravet på säkerhet ska den personuppgiftsansvarige kunna förvissa sig om att personuppgiftsbiträdet kan genomföra de säkerhetsåtgärder som måste vidtas och se till att personuppgiftsbiträdet verkligen vidtar åtgärderna (31 § andra stycket PuL). Den personuppgiftsansvarige har alltså ansvar för att kontrollera att biträdet både kan utföra och också faktiskt vidtar lämpliga säkerhetsåtgärder.

Den personuppgiftsansvarige har i förhållande till den registrerade ett fortsatt skadeståndssanktionerat ansvar för att personuppgiftslagen följs vid personuppgiftsbehandlingen hos personuppgiftsbiträdet. Den personuppgiftsansvarige kan således uppdra den faktiska behandlingen av personuppgifterna till biträdet, men aldrig avsäga sig personuppgiftsansvaret. Det är ytterst den personuppgiftsansvarige som ansvarar för att personuppgiftsbehandlingen sker lagenligt och som därför kan bli skadeståndsskyldig gentemot en enskild vid biträdets felaktiga hantering. I förhållande till den registrerade har personuppgiftsbiträdet inget direkt ansvar för personuppgiftsbehandlingens lagenlighet. Det är en annan sak att biträdet kan bli skadeståndsskyldigt gentemot den personuppgiftsansvarige för eventuella brott mot dennes instruktioner, men då på kontraktsrättslig grund och alltså inte i enlighet med personuppgiftslagens skadeståndsregel.

Ett personuppgiftsbiträdesavtal innebär inte med nödvändighet att det angivna biträdet vid en rättslig prövning verkligen befinns vara personuppgiftsbiträde i personuppgiftslagens mening. Det krävs att det faktiskt förhåller sig på det viset, dvs. att biträdet behandlar uppgifter bara i enlighet med instruktioner från den personuppgiftsansvarige. Kammarrätten i Stockholm har i ett avgörande underkänt ett personuppgiftsbiträdesavtal eftersom den personuppgifts-

ansvarige och biträdet rent faktiskt inte behandlade personuppgifter för samma ändamål. ”Biträdets” behandling kunde därför inte anses ske för den personuppgiftsansvariges räkning (dom 2013-10-29, mål nr 2757-13).

Personuppgiftsansvar inom det allmänna

I personuppgiftslagens definition anges alltså inte på motsvarande sätt som i dataskyddsdirektivet vad för slags aktör som kan vara personuppgiftsansvarig. Det förhållandet att personuppgiftsansvaret är skadeståndssanktionerat torde emellertid innebära att ansvaret ytterst måste bäras av ett rättssubjekt, dvs. en fysisk eller juridisk person som kan svara vid domstol och ikläda sig eller åläggas en rättslig skyldighet, t.ex. den att utge skadestånd.

I det allmännas verksamhet anses det dock normalt vara en statlig eller kommunal myndighet som är personuppgiftsansvarig för personuppgiftsbehandlingen snarare än den juridiska personen – staten, landstinget eller kommunen – i vart fall under förutsättning att myndigheten är så självständig att den är en förvaltningsmyndighet. I flertalet registerförfattningar som reglerar personuppgiftsansvaret är det vidare myndigheter som pekats ut som personuppgiftsansvariga trots att de alltså inte utgör egna rättssubjekt i rättslig mening.

Det förhållandet att statliga och kommunala myndigheter inte utgör juridiska personer innebär bl.a. att skadeståndstalan på grund av en myndighets behandling i strid med personuppgiftslagen måste väckas gentemot den juridiska personen, dvs. staten, landstinget eller kommunen.

I ett avgörande av JK rörande krav på skadestånd enligt 48 § PuL på grund av att en länsstyrelse hade registrerat en felaktig uppgift om körkortsspärr i vägtrafikregistret, uppkom fråga om vilken av de inblandade statliga myndigheterna som skulle betala skadeståndet, Vägverket i egenskap av personuppgiftsansvarig för registret eller länsstyrelsen såsom den myndighet som hade gjort den felaktiga inmatningen. JK konstaterade att det är staten som är ersättningsskyldig samt att om flera enheter inom staten är berörda, bör fördelningen av ansvaret myndigheterna emellan bli en fråga för staten själv. Därvid tillämpade JK den principen att ersättningen

skulle utges av den enhet som bar huvudansvaret för felet, i det aktuella fallet länsstyrelsen (JK 2006-09-12, dnr 1127-05-42).

Personuppgiftsbiträden inom det allmänna

Det är inte ovanligt att myndigheter anlitar personuppgiftsbiträden, t.ex. en servicebyrå eller en konsult, för att utföra personuppgiftsbehandlingar för myndighetens räkning (se t.ex. JO 2012/13 s. 362 om Försäkringskassans personuppgiftsbiträdesavtal med Demoskop). På senare år har användning av s.k. molntjänster blivit vanligare, inte minst i kommunal förvaltning, vilket innebär att det måste träffas personuppgiftsbiträdesavtal med leverantören av tjänsten.

Vad särskilt gäller molntjänster har Datainspektionen i ett informationsblad närmare behandlat vad beställare av en molntjänst måste klargöra i avtalet med ett personuppgiftsbiträde. Utöver vad som direkt framgår av personuppgiftslagen och vad som nämnts ovan om underbiträden framhålls bl.a. att det ska finnas tekniska och praktiska förutsättningar att utreda misstankar om att någon hos personuppgiftsbiträdet haft obehörig åtkomst till personuppgifterna och att parterna vet vilka åtgärder som ska vidtas vid avtalets upphörande så att personuppgiftsbiträdet inte har åtkomst till personuppgifterna därefter.

Det förekommer också att myndigheter behandlar personuppgifter som personuppgiftsbiträden åt andra myndigheter. Inte sällan handlar det då om utkontraktering av it-drift från en myndighet till annan myndighet som tillhandahåller it-baserade funktioner. Vidare förekommer det att myndigheter är personuppgiftsbiträde åt enskilda.

Inom hälso- och sjukvårdens olika system för sammanhållen journalföring m.m. synes det vara särskilt vanligt med personuppgiftsbiträdesavtal där en myndighet uppträder som personuppgiftsbiträde i ganska komplicerade konstellationer på olika nivåer och med t.ex. underbiträden till personuppgiftsbiträden på sätt som påminner om stora entreprenadförhållanden (SOU 2014:23 s. 212).

Sveriges Kommuner och Landsting har utformat en mall för personuppgiftsbiträdesavtal i samband med sammanhållen journalföring där personuppgiftsansvariga (t.ex. privata vårdgivare som har avtal om skattefinansierad vård med ett landsting) ger fullmakt för

biträdet (landstinget) att träffa avtal med underbiträden (t.ex. it-leverantörer). Mallen synes vara utformad utifrån Datainspektionens vägledande uttalande. Sveriges Kommuner och Landsting har vidare i en vägledning om molntjänster i skolan utformat rekommendationer om vad personuppgiftsbiträdesavtal med molnleverantörer minst ska innehålla. Innebär molntjänster att personuppgifter lagras i tredjeland, dvs. utanför EU och EES, måste det, med vissa undantag, också finnas ett kontrakt med sådana standardavtalsklausuler som EU-kommissionen utformat för överföring av personuppgifter till ett personuppgiftsbiträde i tredjeland (jfr 13 § PuF).

Som framgått ovan är det den personuppgiftsansvarige och inte personuppgiftsbiträdet som gentemot registrerade bär det skadeståndssanktionerade ansvaret för lagenligheten i behandlingen. Detta gäller alldeles oavsett om det är en myndighet som är personuppgiftsbiträde. Däremot har en myndighet som behandlar personuppgifter i egenskap av personuppgiftsbiträde ett direkt ansvar att följa andra i sammanhanget relevanta författningsbestämmelser, exempelvis regleringen i 2 kap. TF, offentlighets- och sekretesslagen, arkivlagen, förvaltningslagen m.m. Det ansvaret torde inte i sig påverkas av huruvida myndighetens personuppgiftsbehandling sker i rollen som personuppgiftsbiträde eller som personuppgiftsansvarig och det är inte heller ett ansvar som kan bli föremål för avtalskonstruktioner av något slag.

När en myndighet anlitar personuppgiftsbiträden för att behandla personuppgifter måste myndigheten, för det fall personuppgifterna omfattas av sekretess, göra en noggrann bedömning av om sekretessen utgör ett hinder för ett sådant arrangemang. JO har belyst denna fråga i ett beslut i vilket allvarlig kritik riktades mot vårdgivare för att i strid mot hälso- och sjukvårdssekretessen ha lämnat ut patientuppgifter till anställda vid ett företag med vilket man ingått personuppgiftsbiträdesavtal om utförande av läkarsekreterartjänster för journalföring (beslut 2014-09-09, dnr 3032-2011).

E-delegationen har i delbetänkandet Så enkelt som möjligt för så många som möjligt – Bättre juridiska förutsättningar för samverkan och service (SOU 2014:39) behandlat sekretessfrågor i samband med att en myndighet tillhandahåller it-drift åt en annan myndighet. Vidare behandlas vad som gäller i sekretesshänseende när en myndighet tillhandahåller e-tjänster i form av s.k. elektroniska förvar – t.ex. e-tjänsten Mina meddelanden – åt enskilda eller s.k. pre-

sentationstjänster som sammanställer uppgifter från den egna myndigheten eller annan för visning för en enskild.

Närmare om personuppgiftsansvarets räckvidd

Vem som är personuppgiftsansvarig för en viss behandling av personuppgifter är en fråga som ibland kan vara svår att besvara. Det som ska bedömas är vem som bestämmer över ändamålen och medlen för personuppgiftsbehandlingen och det är de faktiska omständigheterna i det enskilda fallet som är avgörande. Olika avtalskonstruktioner där personuppgiftsansvaret preciseras kan beaktas i bedömningen men avgörande är alltid vem (eller vilka) som faktiskt har bestämt över personuppgiftsbehandlingen (Öman/ Lindblom, s. 93).

Det finns exempel i praxis på att domstol, efter en bedömning av hur det faktiskt förhållit sig med bestämmanderätten över ändamål och medel, bortsett från ett upprättat personuppgiftsbiträdesavtal mellan myndigheter. Förvaltningsrätten i Stockholm prövade om ett universitet var personuppgiftsansvarig eller personuppgiftsbiträde avseende en viss datatjänst, Svensk nationell datatjänst, SND. I SND hanterades forskningsdata vari ingick bl.a. personuppgifter som kom från andra forskningshuvudmän än universitetet. Ett personuppgiftsbiträdesavtal fanns enligt vilket universitetet var personuppgiftsbiträde till de olika forskningshuvudmännen när det gällde personuppgifterna i SND. Förvaltningsrätten fann dock, efter en bedömning av omständigheterna, att universitetet inte hanterade uppgifterna efter instruktioner från forskningshuvudmännen utan i själva verket bestämde över ändamålen med och medlen för behandlingen. Universitet befanns därför vara personuppgiftsansvarigt trots personuppgiftsbiträdesavtalet (dom 2013-10-14, mål nr 9987-12).

Att identifiera vem eller vilka bland flera möjliga aktörer som är personuppgiftsansvarig kan alltså ibland vara komplicerat. En annan dimension på ansvarsfrågan som kan vålla svårigheter är att slå fast vad personuppgiftsansvaret i olika delar omfattar. Övergripande frågor såsom anordnande och administration av tekniska informationssystem och liknande kan t.ex. vara relevanta för bedömningen av vem som bestämmer över medlen för personuppgiftsbehandlingen.

Detta i sin tur kan alltså leda till svårigheter att bedöma hur personuppgiftsansvaret allmänt sett ska avgränsas eller vilken räckvidd personuppgiftsansvaret ska anses ha i ett enskilt fall.

EU-domstolen har i mål C-131/12 Google Spain bedömt bl.a. frågan om personuppgiftsansvar såvitt avser publicering av personuppgifter på webbplatser och sökmotorleverantörers verksamhet. En spansk tidning hade år 1998 publicerat vissa personuppgifter om en person i upplagor som sedermera kommit att återpubliceras elektroniskt på internet. Den registrerade ansåg att uppgifterna inte längre borde finnas med i resultaten från en sökning med Googles sökmotor på hans namn.

EU-domstolen konstaterade att sökmotorer spelade en avgörande roll vid den totala spridningen av uppgifterna genom att göra dem tillgängliga för varje internetanvändare som gör en sökning på en persons namn. Enligt domstolen kan den organisering och aggregation av information publicerad på internet som görs av sökmotorerna i syfte att göra det enklare för användarna att få tillgång till informationen – när sökningen efter informationen görs utifrån namnet på en fysisk person – leda till att användarna genom förteckningen över sökresultaten erhåller en strukturerad översikt av information på internet rörande denna person, vilken gör det möjligt för dem att bilda sig en mer eller mindre detaljerad uppfattning av den berörda personen. En sökmotorleverantörs verksamhet kan således på ett betydande sätt, och utöver vad som redan skett genom webbplatsutgivarnas verksamhet, påverka grundläggande rättigheter avseende privatlivet och skyddet för personuppgifter. Därför måste sökmotorleverantören, i egenskap av person som bestämmer ändamålen och medlen för behandlingen av personuppgifter, inom ramen för sitt ansvar, sin behörighet och sina möjligheter säkerställa att verksamheten uppfyller kraven i direktiv 95/46 för att de garantier som föreskrivs i direktivet ska få full verkan och för att ett effektivt och fullständigt skydd för de berörda personerna ska kunna förverkligas, bland annat när det gäller deras rätt till respekt för privatlivet. Enligt EU-domstolen skulle därför artikel 2 b och 2 d i dataskyddsdirektivet tolkas dels så, att en sökmotors verksamhet – som består i att lokalisera information som har publicerats eller lagts ut på internet av tredje män, indexera den på automatisk väg, lagra den tillfälligt och slutligen ställa den till förfogande för internetanvändare enligt en viss prioriterings-

ordning – ska anses utgöra ”behandling av personuppgifter” i den mening som avses i artikel 2 b, när informationen innehåller personuppgifter, dels så, att sökmotorleverantören ska anses vara ”registeransvarig”, dvs. personuppgiftsansvarig, för nämnda behandling av personuppgifter i den mening som avses i artikel 2 d (punkterna 37–41).

Ytterligare en fråga som kan ställas är när i informationshanteringsprocessen personuppgiftsansvaret inträder. Den frågan aktualiserades i rättsfallet HFD 2012 ref. 21. Målet rörde Försäkringskassans elektroniska självbetjäningstjänster via dels en SMS-tjänst för anmälan av tillfällig föräldrapenning, dels en tjänst för arbetsgivares anmälan av anställdas sjukdomsfall, en s.k. Infratjänst. I båda fallen lämnades uppgifter genom elektroniska kommunikationskanaler via olika operatörer och uppgifterna var inte tillgängliga för Försäkringskassan förrän det att de nådde kassans elektroniska mottagningsställe. Frågan i målet gällde om Försäkringskassan skulle betraktas som personuppgiftsansvarig redan innan uppgifterna blev tillgängliga för myndigheten och att myndigheten därför var skyldig att göra en risk- och sårbarhetsanalys avseende de aktuella självbetjäningstjänsterna. Utan att närmare beröra regleringen av personuppgiftsansvaret i tillämplig registerförfattning (dåvarande 6 § lagen [2003:763] om behandling av personuppgifter inom socialförsäkringens administration, numera 114 kap. 6 § SFB) utgick Högsta förvaltningsdomstolen från regleringen i personuppgiftslagen. Domstolen fann att det var Försäkringskassan som hade bestämt såväl ändamålen med behandlingen av personuppgifterna (att göra vissa anmälningar) som medlen för behandlingen (anvisandet av de särskilda kommunikationsvägarna). Enligt domstolen förutsätter personuppgiftsansvar att den som bestämt ändamål och medel för behandlingen också utför behandlingen, dvs. vidtar åtgärder som innefattar behandling enligt 3 § PuL eller att sådana åtgärder utförs för dennes räkning. Även om Försäkringskassan saknade möjligheter att påverka hur uppgifterna hanterades innan de blev tillgängliga för kassan var de åtgärder med personuppgifterna som vidtogs innan de blev tillgängliga att betrakta som ett led i Försäkringskassans behandling av uppgifter i enskilda ärenden. Den omständigheten att Försäkringskassan saknade faktisk möjlighet att påverka hur uppgifterna hanteras innan de blir tillgängliga för myndigheten kunde visserligen innebära svårigheter

vid bedömningen av de skyldigheter och sanktionsmöjligheter som föreskrivs i personuppgiftslagen men detta hindrade inte att kassan hade ansvar för att göra en risk- och sårbarhetsanalys för den aktuella sms-tjänsten. Försäkringskassans personuppgiftsansvar ansågs alltså inträda på ett tidigare stadium än vad som motsvarade Försäkringskassans faktiska kontroll över personuppgifterna.

När flera aktörer är involverade i processer eller informationssystem där personuppgifter behandlas – t.ex. vid interaktiva tjänster på nätet eller i myndighetsövergripande samarbeten – kan det uppkomma frågor kring vem eller vilka som är personuppgiftsansvariga för de olika momenten i hanteringen. Varken dataskyddsdirektivet eller personuppgiftslagen innehåller några bestämmelser till ledning för hur den frågan ska bedömas. I punkt 47 i ingressen till direktivet anges dock att när ett meddelande som innehåller personuppgifter översänds genom förmedling av en organisation för telekommunikation eller elektronisk post, vars enda ändamål är att översända sådana meddelanden, blir det normalt den från vilken meddelandet härrör och inte den som erbjuder den nämnda tjänsten som anses ansvara för behandlingen av personuppgifterna. De som erbjuder sådana tjänster kommer dock normalt att anses som ansvariga för behandlingen av de ytterligare personuppgifter som fordras för att tjänsten ska kunna användas.

Det brukar framhållas att – när flera aktörer är involverade – det är av stor vikt att berörda parter redan innan en tilltänkt personuppgiftsbehandling påbörjas sinsemellan analyserar och klargör hur det förhåller sig med personuppgiftsansvaret för olika moment eller situationer och överväger eventuella personuppgiftsbiträdesfunktioner m.m. (se t.ex. Datainspektionens vägledning för kommuner: Personuppgifter och e-förvaltning, s. 45 f. och SOU 2006:82 s. 342). I sammanhanget kan vidare nämnas att det är ett krav enligt 23–25 §§ PuL att den registrerade får information om vem som är personuppgiftsansvarig för behandlingen av personuppgifter om honom eller henne. Utgångspunkten är alltså att det inte ska förekomma någon personuppgiftsbehandling utan att det är tydligt för den enskilde registrerade vem som är ansvarig. I den mån flera personuppgiftsansvariga är involverade i en och samma personuppgiftsbehandling torde därigenom gälla ett krav på att den enskilde registrerade informeras om hur personuppgiftsansvaret fördelas mellan aktörerna.

Artikel 29-gruppen har behandlat frågor om personuppgiftsansvarets räckvidd och fördelning mellan olika aktörer m.m. i en rapport från 2010 (opinion 1/2010 in the concept of ”controller” and ”processor”, 00264/10/EN WP 169). När det gäller personuppgiftsansvarets fördelning i komplexa situationer med flera inblandade aktörer har gruppen intagit ett ganska flexibelt betraktelsesätt på frågan om personuppgiftsansvar är gemensamt eller uppdelat. I rapporten framhålls att registeransvaret är ett funktionellt begrepp som är avsett att lägga ansvaret där det faktiska inflytandet ligger. Det är de faktiska omständigheterna som ska vara avgörande vid bedömningen. I samarbeten mellan aktörer som delar ändamål och medel för personuppgiftsbehandlingen kan personuppgiftsansvaret vara gemensamt medan samarbeten i form av informationsutbyten mellan aktörer som behandlar personuppgifter för olika ändamål ofta kan ses som överföring av data mellan separata personuppgiftsansvariga. Vid gemensamma infrastrukturer där flera aktörer tillsammans bestämmer medlen för behandling av personuppgifter kan aktörerna vara gemensamt ansvariga för infrastrukturen även om de inte har samma ändamål för sina respektive personuppgiftsbehandlingar för vilka de är separat personuppgiftsansvariga. I rapporten nämns också andra exempel på fall där personuppgiftsansvaret vid olika samarbeten m.m. kan vara delvis gemensamt, delvis uppdelat. Vidare betonas att ansvaret mycket väl kan vara differentierat mellan aktörerna och att olika grader av kontroll kan ge upphov till olika grader av ansvar. Avtalsmässiga villkor och förhållanden mellan aktörerna kan vara användbara vid bedömningen av ansvarets förläggande eller fördelning, särskilt om det inte finns någon anledning att ifrågasätta att avtalet korrekt speglar verkligheten. I komplexa system kan enskilda registrerades rätt till information och andra rättigheter enligt dataskyddsdirektivet tillgodoses på olika nivåer av de olika aktörerna. Särskilt viktigt är dock att efterlevnaden av dataskyddsbestämmelserna och ansvaret för eventuella brott mot bestämmelserna är tydligt fördelade i komplexa behandlingsmiljöer samt att inga situationer uppstår där skyldigheter och rättigheter som följer av dataskyddsdirektivet inte följs av någon av aktörerna. Så länge som fullständig efterlevnad garanteras, bör de inblandade aktörerna ha utrymme till flexibilitet i fördelningen av skyldigheter och ansvar. Den enskilde registrerade måste dock i komplexa behandlingsmiljöer få utförlig information

om de olika aktörerna och personuppgiftsbehandlingens olika moment samt om hur ansvaret för att tillgodose den enskildes rättigheter fördelas mellan aktörerna.

Särskilt om personuppgiftsansvar vid tillgång till uppgifter genom direktåtkomst m.m.

När en myndighet har direktåtkomst till en annan myndighets personuppgifter kan det uppkomma frågeställningar rörande personuppgiftsansvarets avgränsning och räckvidd, exempelvis om hur långt den utlämnande myndighetens ansvar sträcker sig och när den mottagande myndighetens ansvar inträder.

Enligt Datalagskommittén borde den som t.ex. via ett nätverk har åtkomst till och kan läsa och söka bland personuppgifter utan självständig rätt eller faktisk möjlighet att ändra, komplettera eller radera uppgifterna normalt inte anses vara personuppgiftsansvarig (SOU 1997:39 s. 334). En sådan begränsad tillgång innebär nämligen ingen bestämmanderätt över ändamål och medel som förutsätts för personuppgiftsansvar. Om denne dock med eller utan rätt faktiskt börjar bestämma över ändamålen och medlen genom att t.ex. ändra, komplettera eller radera bland uppgifterna, inträder dock ett personuppgiftsansvar. Samma ståndpunkt har Datainspektionen framfört i ett informationsblad om personuppgiftsansvar (Datainspektionens informationsblad november 1999, uppdaterad januari 2008, se även t.ex. prop. 2007/08:126 s. 61 f.).

I litteraturen har framhållits att den som gör en databas med personuppgifter tillgänglig för tredje man via nätverk eller annan teknisk förbindelse (s.k. online-tjänst) är ensam personuppgiftsansvarig för den behandling av personuppgifter som de utomståendes sökningar och bearbetningar av databasen innebär, men inte för de vidare behandlingar som de utomstående kan komma att utföra avseende de insamlade personuppgifterna (Öman/Lindblom, s. 97).

En utlämnande myndighet kan knappast undgå att vara personuppgiftsansvarig för det utlämnande som åtgärden att göra personuppgifterna tillgängliga för annan innebär. Det kan vidare konstateras att en myndighets direktåtkomst till en annan myndighets uppgiftssamlingar inte med automatik medför något personuppgiftsansvar för sådan personuppgiftsbehandling som sker när en befattningshavare hos en mottagande myndighet i ett enskilt fall tar

del av uppgifter i uppgiftssamlingen. Den gängse uppfattningen torde vara att det då är den utlämnande myndigheten som är personuppgiftsansvarig, i vart fall så länge som den mottagande myndigheten inte kan komplettera eller ändra uppgifterna.

Däremot förefaller det klart att en mottagande myndighet som laddar ned och sparar en kopia av uppgifterna som införlivas i de egna informationssamlingarna i vart fall senast i och med den åtgärden blir personuppgiftsansvarig för den behandling som åtgärden innebär och för den fortsatta behandlingen av uppgifterna. Normalt torde den utlämnande myndigheten inte ha ett kvarstående personuppgiftsansvar för den mottagande myndighetens fortsatta behandling.

10.1.3 Reglering i registerförfattningar

Enligt artikel 2 d i dataskyddsdirektivet kan medlemsstaterna i nationell rätt utse den registeransvarige när ändamålen och medlen för behandlingen bestäms av nationella författningar eller gemenskapsrätten. Denna möjlighet har i Sverige utnyttjats flitigt genom reglering av personuppgiftsansvar i registerförfattningar.

I den mån en registerförfattning har lagform med kompletterande bestämmelser i en anknytande förordning, brukar personuppgiftsansvaret regleras i lagen. Ett undantag härifrån är personuppgiftsbehandlingen inom socialtjänsten där personuppgiftsansvaret reglerats i förordning (6, 11, 17 och 22 §§ förordningen [2001:637] om behandling av personuppgifter inom socialtjänsten).

I vissa fall har regleringen av personuppgiftsansvaret motiverats med att detta ansetts nödvändigt med tanke på att ändamålen anges i lagen i stället för att bestämmas av den aktuella myndigheten. Det har nämligen befarats att tveksamhet annars kan uppstå om huruvida myndigheten verkligen har ett sådant inflytande över ändamålen med behandlingen att den blir att anse som personuppgiftsansvarig vid en tillämpning av personuppgiftslagens regler (se t.ex. Lagrådets synpunkter i prop. 1997/98:80 s. 117 och 1997/98:108 s. 90). Från integritetsskyddssynpunkt har det vidare ofta ansetts lämpligt att på ett tydligt sätt peka ut vem som är personuppgiftsansvarig för den behandling som regleras i en registerförfattning (se t.ex. prop. 2000/01:126 s. 33).

Det vanligaste är att en myndighet som omfattas av en registerförfattning anges som personuppgiftsansvarig för den behandling av personuppgifter ”som myndigheten utför”.

Mindre vanligt är att en myndighet ges ett personuppgiftsansvar även för personuppgiftsbehandling som andra myndigheter utför. När detta förekommer handlar det ofta om renodlade registerförfattningar som reglerar förandet av vissa register. Exempelvis har Lantmäteriet enligt 5 § lagen (2000:224) om fastighetsregister ett ensamt personuppgiftsansvar för fastighetsregistret trots att flera kommunala lantmäterimyndigheter också är registerförande. I motiven diskuterades för- och nackdelar med ensamt respektive uppdelat personuppgiftsansvar. Det uppdelade ansvar som kunde tänkas skulle i så fall bygga på att den myndighet som för in en uppgift i registret också är den som har möjlighet att se till att det sker på ett korrekt sätt och därför borde ansvara för den uppgiften medan Lantmäteriet skulle ges ett övergripande ansvar. Ett sådant uppdelat personuppgiftsansvar ansågs dock ge upphov till ganska komplicerade frågor eftersom införda uppgifter sprids till olika delar av registret på ett sätt som införande kommunal myndighet saknar kontroll över, vilket skulle ha betydelse även för hur långtgående Lantmäteriets övergripande ansvar skulle vara. Ett uppdelat ansvar skulle vidare medföra att det för den enskilde i många situationer skulle framstå som oklart vem han eller hon kunde vända sig till för att utverka sina rättigheter. Ett ensamt ansvar för Lantmäteriet bedömdes därför vara mest fördelaktigt för den enskilde registrerade (prop. 1999/2000:39 s. 81 f.).

I det vi kallar informationshanteringsförfattningar är alltså det normalt förekommande ett uppdelat personuppgiftsansvar i den meningen att det anges att varje myndighet ansvarar för den behandling som den myndigheten utför. Så är t.ex. fallet beträffande Skatteverket, Kronofogdemyndigheten och Tullverket enligt informationshanteringsförfattningarna på området skatt, folkbokföring, exekution och tull. Både Kronofogdemyndigheten och Tullverket har eller får ges direktåtkomst till Skatteverkets beskattningsdatabas. Även socialnämnder kan få sådan direktåtkomst (se 1 kap. 5 § lagen om behandling av uppgifter i Kronofogdemyndighetens verksamhet, 1 kap. 6 § lagen om behandling av uppgifter i Tullverkets verksamhet och 11 § förordningen om behandling av personuppgifter inom socialtjänsten). I förarbetena berördes inte hur

bestämmelserna om personuppgiftsansvar i mottagande myndigheters informationshanteringsförfattningar förhåller sig till Skatteverkets ansvar när Skatteverket lämnar ut personuppgifter till dem via direktåtkomst, dvs. vem som har personuppgiftsansvaret för de konkreta behandlingar som sker då någon av de mottagande myndigheterna gör en sökning i beskattningsdatabasen. Så skedde däremot i förarbetena till kustbevakningsdatalagen (2012:145). Den lagen liknar nyss nämnda informationshanteringsförfattningar på så sätt att den myndighet som omfattas av lagens tillämpningsområde enligt en lagbestämmelse är ”personuppgiftsansvarig för den behandling som myndigheten utför” (2 kap. 4 § kustbevakningsdatalagen). Flera myndigheter har direktåtkomst till Kustbevakningens uppgiftssamlingar. Beträffande frågan om vad som gäller i fråga om personuppgiftsansvar när en annan myndighet använder direktåtkomsten enbart för att läsa en uppgift framhöll regeringen följande (prop. 2011/12:45 s. 199).

> Den myndighet som samlar in och lagrar personuppgifter är personuppgiftsansvarig för den behandlingen. Om samma uppgift lämnas ut till en annan myndighet, genom direktåtkomst eller på något annat sätt, blir den mottagande myndigheten personuppgiftsansvarig för den fortsatta behandlingen hos den myndigheten. När uppgifter lämnas ut till olika myndigheter kan alltså personuppgiftsansvaret för en och samma personuppgift ligga hos flera myndigheter. Var och en av dessa ansvarar för den egna behandlingen.

Frågan om personuppgiftsansvarets fördelning diskuterades tämligen ingående i lagstiftningsärendet rörande personuppgiftsbehandling i verksamhet inom socialförsäkringens administration, dvs. hos Försäkringskassan och Pensionsmyndigheten, numera reglerad i 114 kap. SFB. Enligt 114 kap. 6 § är en myndighet inom socialförsäkringens administration personuppgiftsansvarig för ”den behandling av personuppgifter som den utför”. I förarbetena till bestämmelsen diskuterades frågan om lämpligheten i myndighetsgemensamt personuppgiftsansvar. Till bilden hör att Försäkringskassan vid denna tid ännu inte hade bildats utan det fanns en myndighetsstruktur med Riksförsäkringsverket som central myndighet och ett antal fristående försäkringskassor mellan vilka ansvaret skulle fördelas. Regeringen anförde att det inte var ändamålsenligt att i lag i detalj specificera vem som skulle vara personuppgiftsansvarig för alla de olika typer av behandlingar som kunde tänkas förekomma inom

socialförsäkringens administration. Särskilt gällde detta de mer komplexa förhållanden som rådde vid myndighetsgemensam användning av de stora register som ingår i socialförsäkringsdatabasen. I stället borde personuppgiftsansvaret fördelas genom en regel av mer övergripande karaktär som tog sikte på den myndighet som utför en viss behandling. Enligt regeringen var det den enskilda behandlingen som skulle utgöra grunden för fördelningen av personuppgiftsansvaret. Regeringen fortsatte enligt följande (prop. 2002/03:135 s. 52 f.).

> Har en uppgift lagrats i databasen är det den myndighet som i och för sin verksamhet utför lagringsåtgärden som är ansvarig för att den lagrade uppgiften är korrekt. Ansvaret för uppgiften bör rimligtvis sedan sträcka sig så långt som fram till den tidpunkt då gallring aktualiseras, dock inte längre än fram till den tidpunkt då den myndigheten av olika skäl inte längre besitter möjligheter att förfoga över uppgiften genom rättning, blockering, borttagning etc. Om en personuppgift lämnas ut av en annan myndighet än den som registrerade uppgiften svarar naturligtvis den utlämnande myndigheten för den behandling som utgörs av själva utlämnandet.
>
> För den fortsatta behandlingen av uppgiften efter en registrering kan även andra myndigheter vara ansvariga, allt efter vilka faktiska behandlingar som utförs. Förslaget om fördelning av personuppgiftsansvar förutsätter naturligtvis att det går att genom loggning spåra vilken myndighet som företagit en viss behandling.
>
> I övergripande frågor, såsom ansvar för att tekniska eller organisatoriska säkerhetsåtgärder vidtas, måste personuppgiftsansvaret fördelas efter vilka myndigheter som har befogenhet och skyldighet att utföra dessa åtgärder. I regel torde det följa av åläggandet för Riksförsäkringsverket i verksinstruktionen att vara ansvarig systemägare för Riksförsäkringsverkets och försäkringskassornas gemensamma IT-system att det är verket som har personuppgiftsansvaret vad avser sådana frågor. Enligt regeringens uppfattning innebär det lämnade förslaget i princip ett sådant "gemensamt" personuppgiftsansvar som ett flertal försäkringskassor efterlyst. Att införa en bestämmelse som innefattar begreppet "gemensamt personuppgiftsansvar" är dock inte i sig ägnat att bringa större klarhet rörande fördelningen av personuppgiftsansvaret eftersom det i enlighet med vad som anförts ovan i själva verket är så att personuppgiftsansvaret splittras upp på de olika myndigheterna. Enligt regeringens uppfattning bör personuppgiftsansvaret i stället fördelas utifrån en bestämmelse som tar sikte på vilken myndighet som utför en behandling av personuppgifter.

Även i patientdatalagen (2008:355), en informationshanteringsförfattning som ska tillämpas av en stor mängd personuppgiftsansvariga vårdgivare, finns bestämmelser som fördelar personuppgiftsansvaret. Varje hälso- och sjukvårdsmyndighet ansvarar enligt 2 kap. 6 § för den personuppgiftsbehandling som myndigheten utför. I paragrafen förtydligas att detta även omfattar den behandling av personuppgifter som en myndighet utför när myndigheten genom direktåtkomst i ett enskilt fall bereder sig tillgång till personuppgifter om en patient hos en annan vårdgivare eller hälso- och sjukvårdsmyndighet. Enligt motiven följde i och för sig redan av bestämmelsen om att var och en ansvarar för den behandling som man själv utför att den vårdgivare (eller myndighet) som använder en direktåtkomst för att söka efter eller läsa vårddokumentation hos annan vårdgivare blir personuppgiftsansvarig för den behandling som detta innebär. Datainspektionen hade emellertid i sitt remissvar anfört att en sådan skillnad mot vad som normalt anses gälla vid direktåtkomst borde kunna utläsas i lagen. Av den anledningen ansåg regeringen att ett förtydligande borde införas i bestämmelsen (prop. 2007/08:126 s. 61 f. och s. 230).

Av intresse är vidare bestämmelsen i 6 kap. 6 § patientdatalagen om att regeringen eller den myndighet regeringen bestämmer vid sammanhållen journalföring med direktåtkomst över vårdgivare- eller myndighetsgränser får meddela föreskrifter om vem som ska ha personuppgiftsansvar för övergripande frågor om tekniska och organisatoriska säkerhetsåtgärder. Den möjligheten öppnar således för en reglering som separerar olika moment i personuppgiftsansvaret. Som huvudregel gäller dock även vid direktåtkomst genom sammanhållen journalföring att varje vårdgivare eller myndighet är personuppgiftsansvarig för den behandling som den utför. I motiven framhöll regeringen att beroende på organisation och samarbetsformer vid olika system för sammanhållen journalföring torde regeln i 2 kap. 6 § ofta innebära ett solidariskt personuppgiftsansvar för övergripande frågor. En sådan ordning framstår dock inte alltid som naturlig. Om exempelvis allas vårddokumentation lagras och behandlas i en gemensam databas som administreras av bara en av vårdgivarena, t.ex. ett landsting – som också i praktiken dikterar villkoren för de andra vårdgivarnas deltagande i systemet – kan det tala för att det aktuella landstinget bör anses ha ett personuppgiftsansvar för övergripande frågor. Eftersom det vidare inte

alltid är helt klart hur det förhåller sig med personuppgiftsansvaret i övergripande frågor vid gränsöverskridande personuppgiftsbehandling, kan det dessutom finnas ett behov av en tydlig reglering i dessa frågor. Därför befanns det finnas ett behov av det aktuella bemyndigandet för regeringen (prop. 2007/08:126 s. 255).

Några sådana föreskrifter som avses i 6 kap. 6 § patientdatalagen om personuppgiftsansvar för övergripande tekniska och organisatoriska säkerhetsåtgärder har emellertid hittills inte meddelats. I stället synes förekomma att samarbetande landsting och ingående vårdgivare träffar personuppgiftsbiträdesavtal om att landstinget utför viss behandling för de övriga vårdgivarnas räkning såsom biträde.

I sitt slutbetänkande har Utredningen om rätt information i vård och omsorg (SOU 2014:23) föreslagit att bemyndigandet avskaffas. Enligt utredningen är det av flera skäl olämpligt eller mindre ändamålsenligt att regeringen fattar beslut om personuppgiftsansvaret, bl.a. eftersom bemyndigandet bidrar till passivitet hos vårdgivarna själva. För att stimulera vårdgivarna att själva aktivt analysera och ta ställning till frågan om någon eller några ska ha ett personuppgiftsansvar för övergripande säkerhetsfrågor har utredningen föreslagit en grundläggande bestämmelse som anger att vårdgivare som utbyter uppgifter genom direktåtkomst eller på annat sätt samverkar vid behandling av personuppgifter, genom överenskommelse ska tydliggöra hur personuppgiftsansvaret är fördelat med avseende på övergripande tekniska och organisatoriska säkerhetsåtgärder.

I förslaget till domstolsdatalag (Ds 2013:10) föreslås att Domstolsverket – som utvecklar och tillhandahåller det verksamhetssystem som alla domstolar arbetar i – ska vara personuppgiftsbiträde åt var och en av domstolarna såsom personuppgiftsansvariga för den behandling av personuppgifter som varje domstol i fråga utför. Förslaget innebär att domstolarna får teckna skriftliga personuppgiftsbiträdesavtal med Domstolsverket.

10.1.4 Våra överväganden och förslag

En myndighet ska vara personuppgiftsansvarig för den behandling som myndigheten utför

> **Förslag:** I den nya lagen införs en generell regel som innebär att en myndighet alltid är personuppgiftsansvarig för den behandling som myndigheten utför.

Som har framgått får utgångspunkten enligt den unionsrättsliga dataskyddsregleringen anses vara att de faktiska förhållandena i det enskilda fallet ska vara avgörande när personuppgiftsansvarets omfattning och fördelning ska bestämmas. Genom att ansvaret förläggs till den eller de som utifrån förutsättningarna i det enskilda fallet faktiskt bestämmer över ändamål och medel skapas garantier för att det också finns en reell förmåga att leva upp till de skyldigheter som ansvaret är förknippat med. Att utgå från de faktiska förhållandena snarare än organisatoriska eller rättsliga faktorer är också ägnat att i varje enskilt fall åstadkomma ett heltäckande skydd som eliminerar risken för att någon skyldighet eller rättighet "faller mellan stolarna". Definitionen av personuppgiftsansvarig i 3 § PuL kan sägas ge uttryck för detta.

Enligt vår uppfattning bör samma utgångspunkter gälla även då myndigheter behandlar personuppgifter, dvs. att de faktiska förhållandena i det enskilda fallet ska avgöra både när en myndighets personuppgiftsansvar uppstår eller upphör och huruvida detta ansvar, då flera aktörer samverkar, ska vara gemensamt eller uppdelat på något sätt.

Det är enligt personuppgiftslagen den som bestämmer bl.a. ändamålen med en behandling som är personuppgiftsansvarig. När ändamål för behandling är reglerade i författning är det därför naturligt att också personuppgiftsansvaret regleras. Annars kunde det uppstå tveksamheter kring frågan om en myndighet verkligen bestämmer ändamål och medel för personuppgiftsbehandlingen. Vi har i avsnitt 9.2.4 föreslagit att myndigheter som huvudregel själva ska, utifrån de uppgifter respektive myndighet har, formulera särskilda, uttryckliga och berättigade ändamål som grund för att över huvud taget samla in information som sedan behandlas i myndighetens verksamhet. Eftersom det med vårt förslag alltså normalt

sett inte ska förekomma några ändamålsbestämmelser finns det inte anledning att av det skälet införa regler om personuppgiftsansvar. Frågan blir då om det av något annat skäl finns anledning att i den generella lagen införa bestämmelser som särreglerar personuppgiftsansvaret eller om det enbart ska hänvisas till definitionen i 3 § PuL som anger hur ansvaret ska identifieras.

I flertalet informationshanteringsförfattningar som är konstruerade på det sättet att de inom sitt respektive tillämpningsområde reglerar mer än en myndighets personuppgiftsbehandling anges att varje myndighet är personuppgiftsansvarig för den behandling som myndigheten utför.

Vi menar att det i en generell reglering om myndigheters behandling av personuppgifter är lämpligt att på motsvarande sätt genom en uttrycklig bestämmelse klargöra att det är den faktiska informationshantering som sker i en viss myndighets verksamhet som ska vara utgångspunkten för bedömningen. En sådan bestämmelse, som alltså ska föreskriva att en myndighet är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför, innebär att de faktiska förhållandena får en större betydelse än vad som hade varit fallet med enbart en hänvisning till personuppgiftslagen eftersom det då inte behöver ske någon prövning av huruvida myndigheten i fråga bestämt ändamålen och medlen för behandlingen i fråga. Visserligen kan man utgå från att en myndighet bestämmer både ändamålen och medlen för den personuppgiftsbehandling som sker hos myndigheten. Det kan dock inte uteslutas att det någon gång kan uppstå tveksamheter rörande denna fråga. Redan detta talar för att myndighetens ansvar för personuppgiftsbehandlingen bör följa direkt av den nya lagen.

En grundregel om att en myndighet är ansvarig för den behandling av personuppgifter som myndigheten utför har emellertid sin främsta betydelse genom att den – då flera aktörer samarbetar eller det annars kan finnas någon alternativt tänkbar personuppgiftsansvarig – pekar ut vem som är ansvarig för varje enskild urskiljbar personuppgiftsbehandling. Enligt vår uppfattning talar tungt vägande skäl för att personuppgiftsansvaret för en enskild behandling bör förläggas hos den som har faktisk möjlighet att påverka om och hur behandlingen ska utföras, dvs. hos den som utför den. Vi föreslår därför en sådan grundregel.

Den föreslagna grundregeln är, enligt vår mening, fullt förenlig med dataskyddsdirektivet. Den innebär som vi ser det inte ett sådant rättsligt utpekande av den registeransvarige som enligt direktivet förutsätter att ändamålen regleras på motsvarande vis utan bör ses som ett förtydligande av hur innebörden i direktivets huvudregel om registeransvar ska förstås på myndighetsområdet.

Grundregeln undanröjer emellertid på inget sätt svårigheterna kring avgränsningen av personuppgiftsansvaret. En komplicerande faktor här är t.ex. att det inte alltid är så lätt att avgöra vad som utgör en behandling i förhållande till en annan. I komplexa informationsmiljöer kan det tänkas att samma uppgift behandlas i olika skeden av flera aktörer i processer som inte så lätt kan avgränsas, i vart fall inte utifrån rättsliga principer. Samtidigt går det enligt vår mening inte att införa bestämmelser som anger fixerade gränser för när en myndighets personuppgiftsansvar börjar eller slutar och exakt vad detta under mellantiden omfattar. Sådana rättsliga gränsdragningar kan knappast utformas på ett sätt som skulle kunna fungera tillfredsställande i praktisk tillämpning. Avgränsningen måste därmed även i fortsättningen ske genom att analysera och bedöma de närmare faktiska förhållandena. För integritetsskyddet är det dock centralt att personuppgiftsansvaret inte är otydligt och att komplicerade fall hanteras så att enskilda informeras och vägleds på tillfredsställande sätt. Det är också väsentligt att olika behandlingar dokumenteras så att personuppgiftsansvaret för specifika behandlingar kan identifieras i efterhand.

I sammanhanget kan vidare påpekas att det är av grundläggande betydelse för integritetsskyddet att det i myndighetens personuppgiftsansvar ingår att se till att det inom myndigheten finns en organisation, instruktioner och myndighetsintern praxis som möjliggör kontroll och styrning av den personuppgiftsbehandling som sker, vilket i sin tur är nödvändigt för att myndigheten ska kunna upptäcka och åtgärda eventuella brister i sin behandling av personuppgifter (jfr JO:s beslut den 17 mars 2015, dnr. 5205-2013, rörande det s.k. Kringresanderegistret vid dåvarande Polismyndigheten i Skåne).

Personuppgiftsansvar vid direktåtkomst m.m.

Förslag: I lagen införs en bestämmelse som klargör att personuppgiftsansvaret för behandling som myndigheten utför även omfattar sådan behandling som utförs när myndigheten via direktåtkomst hos en annan myndighet eller enskild behandlar en tillgängliggjord personuppgift.

Innan en utlämnande myndighet medger en annan myndighet eller enskild direktåtkomst till personuppgifter ska de komma överens om hur skyddet för personuppgifterna ska säkerställas. Överenskommelsen ska i första hand syfta till att klargöra ansvarsförhållandena mellan samarbetsparterna. Av överenskommelsen ska framgå hur utövandet av de skyldigheter som personuppgiftsansvaret innefattar ska ske. Motsvarande ska gälla vid andra former av informationsutbyten som innebär behandling av personuppgifter i gemensamma eller annars integrerade informationssystem.

Personuppgiftsansvar för urskiljbara behandlingar

En särskild fråga är vad som ska gälla för enstaka behandlingar vid direktåtkomst. Direktåtkomst är en speciell form av elektroniskt utlämnande vars innebörd vi närmare behandlat i kapitel 5. Där har vi gjort bedömningen att den begreppsmässiga åtskillnaden mellan direktåtkomst och annat elektroniskt utlämnande bör behållas. Såsom vi tidigare konstaterat innebär direktåtkomst att olika myndigheter samtidigt utför behandlingar av personuppgifter i en informationssamling som genom åtkomsten i viss mån blir i rättslig mening gemensam. Både den utlämnande och mottagande myndigheten utför behandlingar men på olika nivåer.

Av den nyss föreslagna grundregeln följer att en myndighet som har tillgång till en annan myndighets personuppgifter via direktåtkomst blir personuppgiftsansvarig för den behandling som utförs då direktåtkomsten används, exempelvis när en sökning hos den utlämnande myndigheten sker. Detta innebär en avvikelse från vad som enligt gängse uppfattning torde följa av en tillämpning av personuppgiftslagen, nämligen att den som har direktåtkomst med möjlighet att endast söka och läsa inte blir personuppgiftsansvarig

för den behandling som detta innebär. I ett tidigare lagstiftningsärende har det ansetts finnas behov av ett klargörande rörande detta (2 kap. 6 § patientdatalagen, prop. 2007/08:126 61 f.). Enligt vår uppfattning vinner den av oss föreslagna lagen i tydlighet med en motsvarande bestämmelse. Vi föreslår därför en sådan.

Vid direktåtkomst har den utlämnande myndigheten givetvis ett personuppgiftsansvar för innehållet i sin informationssamling och för att tillgängliggörandet av personuppgifter sker på ett lagligt sätt. Detta ansvar omfattar även den fortsatta lagringen och det kontinuerliga tillgängliggörandet för externa mottagare. Detta är en följd av grundregeln om att en myndighet ansvarar för den behandling som myndigheten utför. Något ”medansvar” uppstår enligt vår mening inte hos den mottagande myndigheten bara för att denna har en latent möjlighet att själv ta fram personuppgifter ur informationssamlingen och då ansvarar för den behandling som detta innebär.

Det förekommer, som har framgått ovan, författningar rörande viss registerföring, t.ex. beträffande lägenhetsregistret, där personuppgiftsansvaret samlats hos den centrala förvaltaren av registret och där andra myndigheters användning av registret omfattas av registerhållarens personuppgiftsansvar. Det kan inte uteslutas att en sådan ordning av olika skäl kan visa sig vara en lämplig ordning även om den generella lagen avses vara tillämplig i övrigt. Inget hindrar att det i ett sådant fall genom särskild reglering för en viss myndighet eller verksamhet görs avsteg från den huvudregel vi föreslår. Sådana regler kan då, beroende på omständigheterna, endera tas in i en till den nya lagen anknytande bilaga eller förordning eller i annan särskild författning.

Krav på överenskommelser om hur skyddet för personuppgifterna ska säkerställas

I personuppgiftsansvaret ligger inte bara att urskiljbara faktiska behandlingar ska ske i enlighet med de grundläggande kraven i 9 § PuL och att personuppgifter bara behandlas när det är tillåtet m.m. Ansvaret omfattar även mer övergripande frågor såsom att se till att behandlade personuppgifter skyddas genom tekniska och organisatoriska säkerhetsåtgärder. Vidare innebär det bl.a. en skyldighet

att självmant respektive på begäran ge registrerade information om behandlingen och att rätta eller ta bort felaktiga uppgifter.

Vi har kunnat konstatera att det föreligger en viss variationsrikedom när det gäller de närmare tekniska och administrativa förutsättningarna vid myndigheters elektroniska informationsutbyten. Direktåtkomst kan t.ex. avse extern tillgång till en databas som finns hos en utlämnande myndighet. Direktåtkomst kan emellertid också handla om sammankopplade informationssystem med olika informationssamlingar där medverkande myndigheter samtidigt är både utlämnare av egen information och mottagare av andra myndigheters. Om och i så fall när personuppgiftsansvaret för mer övergripande frågor övergår från den ena aktören till den andra eller om personuppgiftsansvaret är gemensamt kan, som vi har konstaterat ovan, knappast regleras utan måste primärt bli en fråga för de inblandade aktörerna att bedöma. Avgörande är då vem eller vilka som har faktiska förutsättningar, befogenheter och förmåga att påverka behandlingen.

Oavsett vilket slags system för åtkomst som ett informationsutbyte bygger på är det alltså av stor vikt för integritetsskyddet att frågor om personuppgiftsansvarets fördelning och hur personuppgifterna ska skyddas genom tekniska och organisatoriska säkerhetsåtgärder är grundligt analyserade och utredda innan åtkomsten etableras. Detta gäller i synnerhet vid direktåtkomst. Ju mer komplext ett system för informationsutbyte är, desto noggrannare måste de involverade myndigheterna och eventuella enskilda aktörerna ha tänkt igenom formerna för samarbetet. Det kan handla om frågor om t.ex. vem som ska ansvara för olika funktioner eller moment, säkerhetslösningar, loggning, kontroller och liknande eller om ansvaret för detta ska vara gemensamt. Särskilt viktigt är att aktörerna redan på förhand tillsammans utreder och klargör hur en heltäckande efterlevnad av samtliga dataskyddsbestämmelser ska garanteras så att det inte uppstår situationer där de olika skyldigheterna inte följs av någon av aktörerna eller där den registrerade blir hänvisad fram och tillbaka. Däremot finns det inget hinder mot att enskilda registrerades rätt till information och andra rättigheter tillgodoses på olika nivåer och av olika aktörer. Det är vår bedömning att direktivet möjliggör ett utrymme för flexibilitet i fördelningen av det praktiska ombesörjandetav skyldigheter och ansvar så länge som erforderligt skydd garanteras. Den enskilde

registrerade måste dock i komplexa behandlingsmiljöer få utförlig information om de olika aktörerna och personuppgiftsbehandlingens olika moment samt om hur ansvaret för att tillgodose den enskildes rättigheter fördelas mellan aktörerna.

Vi instämmer i vad Utredningen om rätt information i vård och omsorg påpekat om att det finns betydande fördelar med att frågor om personuppgiftsansvaret vid direktåtkomst i första hand hanteras av de inblandade aktörerna själva, dock att de kan behöva stimuleras till detta genom att det ställs krav på en analys av det planerade samarbetet och att man träffar en överenskommelse om hur personuppgiftsansvaret för tekniska och organisatoriska säkerhetsåtgärder fördelas (SOU 2014:23 s. 206 f.). Enligt vår mening är detta ett generellt behov vid direktåtkomst på myndighetsområdet. Överenskommelser bör emellertid, enligt vår mening, inte enbart avse frågor om hur personuppgifter ska skyddas genom mer eller mindre övergripande tekniska och organisatoriska säkerhetsåtgärder. Även andra skyldigheter som följer med personuppgiftsansvaret bör bli föremål för diskussion och, vid behov, klargöras i överenskommelsen mellan aktörerna. Det kan gälla t.ex. frågor om hur man praktiskt organiserar och eventuellt samordnar rutiner och tjänster för rättelse, information som ska lämnas på begäran av den registrerade eller hur samarbete mellan involverade personuppgiftsombud kan underlättas etc.

Vi föreslår mot den angivna bakgrunden att det införs en bestämmelse som innebär att innan en utlämnande myndighet medger en annan myndighet eller enskild direktåtkomst till personuppgifter, myndigheterna ska komma överens om hur de skyldigheter som följer med personuppgiftsansvaret ska utövas. Övervägande skäl talar för att ansvaret för att en överenskommelse träffas bör ligga på den utlämnande myndigheten. I sådana fall då informationsflödet går åt båda hållen, blir ansvaret för överenskommelsen gemensamt.

Myndigheter och andra aktörer kan emellertid samarbeta på sätt som innefattar behandling av personuppgifter utan att det behöver handla om att en eller flera myndigheter ger eller får direktåtkomst till personuppgifter. Det förekommer andra varianter av informationsutbyten eller samverkan i informationssystem som är gemensamma eller annars integrerade. Till dessa hör bl.a. samarbeten över myndighetsgränser i form av förvaltningsgemensamma e-tjänster som erbjuds eller planeras för enskilda. Exempel härpå är den digi-

tala brevlådan Mina meddelanden och presentationstjänsten Min ärendeöversikt. Vi menar att även vid sådana former av samarbeten som innefattar personuppgiftsbehandling bör det gälla ett krav på att aktörerna i förväg tillsammans klargör ansvarsfördelningen beträffande sådana moment i informationshanteringen som inte kan avgränsas som enskilda urskiljbara behandlingar. Den bestämmelse om att det ska träffas överenskommelser om personuppgiftsansvarets utövande vid direktåtkomst som vi föreslår bör därför även omfatta sådant övrigt samarbete mellan myndigheter eller med enskilda som sker i gemensamma eller annars integrerade informationssystem.

Överenskommelser om personuppgiftsansvarets utövande syftar i första hand till att inblandade aktörer genom ett samarbetsavtal ska ha gjort klart för sig och sinsemellan vara överens om vem eller vilka som ansvarar för olika tekniska eller organisatoriska säkerhetsåtgärder eller andra skyldigheter rörande behandlingen och om hur det ansvaret i praktiken ska realiseras. En överenskommelse har däremot inte någon formell rättsföljd och innebär inget avsteg från principen om att det är de faktiska förhållandena som avgör om och hur personuppgiftsansvaret är fördelat. Det är en annan sak att en sådan överenskommelse naturligen kan komma att få betydelse om personuppgiftsansvaret i efterhand ska identifieras av tillsynsmyndighet eller rättsliga instanser.

Det ska observeras att förslaget om krav på överenskommelser enbart tar sikte på dataskyddsrättsliga frågor om personuppgiftsansvar och skydd för personuppgifter. Vid komplexa myndighetsövergripande samarbeten finns givetvis anledning att i förväg också reda ut andra men näraliggande frågor, t.ex. om hos vilken myndighet upptagningar ska bilda arkiv (jfr 3 § första stycket andra meningen arkivlagen [1990:782]). Frågor av det slaget omfattas inte av vårt förslag om krav på överenskommelse. Kravet torde dock kunna få en indirekt betydelse genom den ”smittoeffekt” på näraliggande frågor som kravet på förberedande risk- och sårbarhetsanalyser och klargöranden av olika ansvarsmoment kan antas få. Det blir naturligt att också reda ut sådana frågor i anslutning till att överenskommelser enligt lagen ska träffas.

Avslutningsvis vill vi påpeka att förslaget om kravet på överenskommelse givetvis inte tar sikte på personuppgifter i register eller annan information som är allmänt tillgänglig för allmänheten, t.ex.

via en myndighets webbplats på internet. Det får anses följa av att det ska vara fråga om mottagares direktåtkomst som ”medges” av den utlämnande myndigheten, dvs. som en mottagare ges genom ett särskilt beslut.

Vi återkommer till den nu föreslagna bestämmelsens utformning i avsnitt 10.2.5.

Särskilt om personuppgiftsbiträden

Förslag: Det som föreskrivs i personuppgiftslagen om att ett personuppgiftsbiträde eller den som arbetar under biträdets ledning bara får behandla personuppgifter i enlighet med den personuppgiftsansvariges instruktioner ska gälla också enligt den nya lagen. Detsamma gäller kravet på att det ska finnas ett skriftligt avtal med personuppgiftsbiträdet liksom kraven på vad avtalet ska innehålla. Utöver detta införs ett krav på att avtalet ska innehålla dokumentation om den personuppgiftsansvariga myndighetens instruktioner till biträdet samt ett förbud mot att biträdet anlitar ett annat biträde, ett underbiträde, utan godkännande från den personuppgiftsansvariga myndigheten. Samma villkor om avtal och instruktioner ska gälla för ett sådant underbiträde. För att skapa ökad tydlighet görs ingen hänvisning till 30 eller 31 § PuL utan regleringen tas in genom särskilda bestämmelser i den nya lagen.

Grundregeln om personuppgiftsansvar och uppdrag som personuppgiftsbiträden

Den av oss föreslagna grundregeln om att en myndighet har personuppgiftsansvaret för den behandling som myndigheten utför har inget direkt samband med frågan om vilka faktiska personuppgiftsbehandlingar som utförs av myndigheten. Förekommer personuppgiftsbiträden kan personuppgiftsansvaret nämligen omfatta betydligt fler faktiska behandlingar än den som sker hos den ansvariga myndigheten.

När en myndighet överlämnar den faktiska behandlingen av personuppgifter till ett personuppgiftsbiträde kvarstår alltså person-

uppgiftsansvaret för myndigheten. Detta kommer till uttryck genom den hänvisning till definitionerna i 3 § PuL som ska gälla även enligt den nya lagen. Av definitionen framgår att personuppgiftsbiträdet bara behandlar personuppgifter för den personuppgiftsansvariges räkning. Det är alltså fortfarande den personuppgiftsansvarige som utför behandlingen i den mening som avses i den bestämmelse om personuppgiftsansvar som vi föreslår även om behandlingen rent faktiskt sker hos biträdet. Av detta följer att om en myndighet agerar som personuppgiftsbiträde åt en annan myndighet eller en enskild, den myndighet där den faktiska behandlingen sker inte är personuppgiftsansvarig för behandlingen.

Som har framgått förekommer biträdeskonstruktioner på det kommunala området, t.ex. inom hälso- och sjukvården vid sammanhållen journalföring. Även inom staten tycks sådana förekomma eller i vart fall har det förutsatts kunna förekomma (se t.ex. SOU 2014:39 och Ds 2013:10).

Avtal mellan myndigheter där en myndighet är personuppgiftsbiträde åt den andra är emellertid en rättslig konstruktion som ter sig tämligen främmande för vad som annars gäller inom den offentliga förvaltningen. Man kan, menar vi, redan från principiella utgångspunkter ställa sig tveksam till att exempelvis två sidoordnade myndigheter träffar den typen av avtal. Det passar inte in i bilden av självständiga myndigheter som inte tar instruktioner från eller låter sig kontrolleras av andra sidoordnade myndigheter. Genom personuppgiftsavtal uppstår befogenheter och lydnadsförhållanden som avviker från vad som annars gäller inom förvaltningen.

Till detta kommer det förhållandet att förvaltningsmyndigheter inte är egna juridiska personer. Rättskapacitet att ingå civilrättsligt bindande avtal tillkommer den juridiska personen, dvs. såvitt är aktuellt nu staten, landstinget eller kommunen. Många myndigheter har i och för sig befogenheter att ingå bindande avtal för statens räkning inom sina respektive verksamhetsområden. Olika enheter, dvs. myndigheter, inom en och samma juridiska person kan dock inte ingå bindande avtal med varandra. Mellan två statliga myndigheter kan således inte träffas avtal i rättslig mening. Motsvarande gäller för kommunala myndigheter inom samma kommun. Att t.ex. statliga myndigheter träffar skriftliga överenskommelser med varandra inom ramen för sina respektive uppdrag och befogenheter är en annan sak.

I artikel 17.3 i dataskyddsdirektivet föreskrivs att ett personuppgiftsbiträdes hantering av personuppgifter ska ske ”genom ett avtal eller genom en annan rättsligt bindande handling mellan registerföraren och den registeransvarige”. Den typ av överenskommelse som kan träffas mellan statliga myndigheter eller mellan kommunala myndigheter i samma kommun torde alltså inte uppfylla direktivets krav på att vara rättsligt bindande. Enligt vår mening innebär detta att en ordning som bygger på att statliga myndigheter på grund av avtal skulle vara personuppgiftsbiträden åt andra statliga myndigheter knappast är en hållbar konstruktion.

Även när myndigheter träffar avtal om att vara personuppgiftsbiträden åt enskilda uppstår en del udda konsekvenser. Enligt personuppgiftslagens regler innebär detta bl.a. att myndigheten i så fall ska arbeta under den enskildes ledning och instruktioner och att den enskilde ska kontrollera myndigheten (30 § första stycket och 31 § andra stycket PuL). Hur det ska gå till i praktiken är höljt i dunkel. Man kan också från principiella utgångspunkter ifrågasätta om en enskild bör kunna träffa avtal med en myndighet som innebär att den enskilde kan bli skadeståndsskyldig gentemot en registrerad för den händelse myndigheten behandlar personuppgifter i strid mot någon relevant bestämmelse. Den här typen av konstruktioner tycks förekomma t.ex. vid sammanhållen journalföring där olika privata vårdgivare är personuppgiftsansvariga med den större och drivande aktören, landstinget, som personuppgiftsbiträde. Personuppgiftsbiträdesavtalet kan därvid vara en del i ett större paket med avtal mellan landstinget och privata vårdgivare om sammanhållen journalföring som i sin tur kan vara en förutsättning för att privata vårdgivare ska kunna få ett sådant vårdavtal med landstinget som innebär att de ingår i den skattefinansierade vården. Styrkeförhållandet mellan den personuppgiftsansvarige och personuppgiftsbiträdet är alltså något annorlunda än det som personuppgiftslagen utgår från. På motsvarande sätt förhåller det sig när t.ex. kommuner ingår personuppgiftsbiträdesavtal om molntjänster med stora multinationella aktörer såsom t.ex. Google.

Vi kan emellertid bara konstatera att det förekommer att myndigheter fungerar som personuppgiftsbiträden. Även om avtalskonstruktionen har inslag som alltså enligt vår mening får en del udda konsekvenser så erbjuder den obestridligen fördelar och möjligheter, även för myndigheter. Det kan alltså antas att anlitande av

myndigheter som personuppgiftsbiträde även i fortsättningen kommer att vara ganska vanligt förekommande och vi ser ingen anledning att föreslå någon förändring av den möjligheten när det gäller avtal mellan myndigheter som hör till olika juridiska personer och mellan myndigheter och enskilda. Detta förutsätter emellertid att eventuella sekretessfrågor kan lösas och att biträdesrelationen kan ske med ett upprätthållande av gränserna mellan myndigheterna och deras respektive informationssamlingar samt mellan myndigheter och enskilda. Här kan särskilt erinras om vikten av att sekretessfrågorna blir grundligt analyserade.

Eftersom myndigheters faktiska behandling av personuppgifter i egenskap av personuppgiftsbiträden inte omfattas av den nya lagens tillämpningsområde saknas behov av någon klargörande bestämmelse om att den grundregel som vi föreslagit om att en myndighet är personuppgiftsansvarig för den personuppgiftsbehandling som myndigheten utför inte gäller då en myndighet bara behandlar personuppgifter för annans räkning såsom personuppgiftsbiträde. Det spelar i det avseendet ingen roll om den personuppgiftsansvarige är en annan myndighet vars personuppgiftsbehandling omfattas av lagens tillämpningsområde. Då blir lagen visserligen indirekt tillämplig på personuppgiftsbiträdets behandling. Adressaten för de olika bestämmelserna i lagen är dock den personuppgiftsansvariga myndigheten och det är den myndigheten som ytterst ansvarar för att lagens bestämmelser följs.

Det finns avslutningsvis skäl att erinra om vikten av att ”biträdesmyndigheten” verkligen behandlar personuppgifterna för den personuppgiftsansvariges räkning och inte själv, trots ett biträdesavtal, bestämmer över ändamålen eller medlen för behandlingen. Oavsett vad ett avtal föreskriver är det de faktiska omständigheterna som är utslagsgivande och det kan alltså inträffa att ”biträdesmyndigheten” i själva verket visar sig vara personuppgiftsansvarig. Det är alltså en fråga för sig huruvida ett påstått personuppgiftsbiträdeskap återspeglar det korrekta förhållandet.

Behövs tydligare regler vad gäller anlitandet av personuppgiftsbiträden?

Dataskyddsdirektivet innebär att det gäller vissa formkrav beträffande anlitandet av personuppgiftsbiträden. Det uppställs krav på att det träffas en bindande överenskommelse. Enligt artikel 17.3 ska registerförarens hantering regleras genom ett avtal eller genom en annan rättsligt bindande handling mellan registerföraren och den registeransvarige. I handlingen ska särskilt föreskrivas dels att registerföraren endast får handla på instruktioner från den registeransvarige, dels att de skyldigheter som anges i artikel 17.1, såsom de definieras i lagstiftningen i den medlemsstat i vilken registerföraren är etablerad, även ska åvila registerföraren. I artikel 17.4 föreskrivs vidare att de delar av avtalet eller den rättsligt bindande handlingen som rör skyddet av uppgifter och de krav som rör åtgärder som anges i artikel 17.1 ska föreligga i skriftlig eller därmed jämförlig form. Syftet är att säkra bevisning.

För att leva upp till direktivets krav måste det som föreskrivs i personuppgiftslagen om att personuppgiftsbiträdet eller den som arbetar under biträdets ledning bara får behandla personuppgifter i enlighet med den personuppgiftsansvariga myndighetens instruktioner gälla också enligt den nya lagen. Detsamma måste gälla kravet på att det ska finnas ett skriftligt avtal med personuppgiftsbiträdet som innehåller föreskrift om biträdets skyldighet att dels bara behandla personuppgifter i enlighet med instruktioner från den personuppgiftsansvarige, dels vidta sådana tekniska och organisatoriska säkerhetsåtgärder som avses i 31 första stycket PuL. Vidare måste föreskrivas att den personuppgiftsansvarige ska vara skyldig att förvissa sig om att personuppgiftsbiträdet kan genomföra de säkerhetsåtgärder som måste vidtas och se till att personuppgiftsbiträdet verkligen vidtar åtgärderna.

Vi har ställt oss frågan i vilken mån det härutöver finns anledning att överväga en reglering som ställer tydligare krav på vad som ska gälla i sammanhanget.

Enligt Datainspektionen har myndigheternas anlitande av personuppgiftsbiträden medfört en utvecklingstrend som innebär att biträdena allt oftare vänder sig till inspektionen med idéer om hur den sammantagna uppgiftsmängden de hanterar – vilken kan omfatta flera personuppgiftsansvarigas uppgifter – kan användas. Det

väcker frågor om hur myndigheterna kan skydda sin information från att användas av biträden samt dessas medarbetare, samarbetspartners eller underbiträden för egna syften som faller utanför biträdesuppdraget. Exempelvis har flera kommuners användning av molntjänster i skolan fått kritik av Datainspektionen för brister i avtalen med molntjänstleverantörer. De påtalade bristerna har t.ex. handlat om bristande instruktioner vad avser för vilka ändamål biträdet får behandla personuppgifter, dvs. inte för egna syften, och vad som ska gälla vid avtalets upphörande. En annan brist är att det inte ställts krav på information om vilka underbiträden som anlitas och var dessa är lokaliserade samt vilka behandlingar de utför.

Visserligen kan överlämnandet av den faktiska personuppgiftsbehandlingen till ett personuppgiftsbiträde många gånger ge ett jämförelsevis bättre skydd genom de kunskapsmässiga, tekniska och administrativa resurser samt kvalificerade infrastruktur som ett sådant biträde inte sällan förfogar över. Enligt vår uppfattning är det emellertid angeläget för förtroendet för myndigheternas informationshantering att anlitandet av personuppgiftsbiträden sker på ett sätt som så långt möjligt eliminerar de risker som kan vara förknippade med att en myndighet avhänder sig den faktiska kontrollen över personuppgifterna.

De bestämmelser som finns i 30 § första stycket och 31 § andra stycket PuL syftar till att ge garantier för att överlämnandet av den faktiska personuppgiftsbehandlingen till ett biträde inte inkräktar på de krav i olika avseenden som personuppgiftslagens hanteringsregler och reglerna om den registrerades rättigheter uppställer. Enligt vår mening bör alltså motsvarande krav gälla även enligt den nya lagen. Detta innebär att den personuppgiftsansvariga myndighetens instruktioner till biträdet måste vara så utformade att det klargörs vad som ska gälla för biträdets hantering. Några närmare bestämmelser om vad instruktionerna ska innehålla ser vi inte något behov av. Förhållandena i det enskilda fallet är här styrande och varierar stort liksom detaljeringsnivån. Instruktioner kan t.ex. gälla hur tillgången till personuppgifter hos biträdets anställda ska minimeras, huruvida och i så fall hur biträdet ska använda krypteringsmetoder vid kommunikation osv.

Däremot anser vi att det kravet borde ställas att en personuppgiftsansvarig myndighets instruktioner till ett personuppgiftsbiträde ska dokumenteras i parternas avtal. Förutom de fördelar

från bevis- och kontrollsynpunkt som ett krav på dokumenterade instruktioner skulle innebära, är det vår uppfattning att det skulle främja utformandet av tydliga och genomtänkta instruktioner som omfattar helheten i den behandling som biträdesavtalet avser. Inte minst det sistnämnda är av stor vikt från dataskyddssynpunkt. Vi föreslår därför att det införs ett krav på att avtalet ska innehålla dokumentation av den personuppgiftsansvariga myndighetens instruktioner.

Enligt vår uppfattning är det vidare inte tillfredsställande att det saknas ett uttryckligt krav på att en personuppgiftsansvarig myndighet måste förvissa sig om att ett personuppgiftsbiträde inte i sin tur överlämnar hela eller delar av personuppgiftsbehandlingen till någon annan utan att myndigheten först informerats, haft tillfälle att överväga frågan och sedan godkänt detta. Indirekt torde ett sådant krav förvisso redan gälla. Att myndigheter i detta avseende bevarar kontrollen över vad som faktiskt sker med personuppgifterna är emellertid av så fundamental betydelse för skyddet av personuppgifterna att det är befogat med ett klargörande i lag. Vi föreslår därför en sådan bestämmelse.

För att skapa en samlad och tydlig reglering föreslår vi ingen hänvisning till bestämmelserna om personuppgiftsbiträden i 30 och 31 §§ PuL utan motsvarande regler angående anlitande av personuppgiftsbiträden bör tas in som bestämmelser i den nya lagen.

10.2 Säkerhet vid behandling av personuppgifter

10.2.1 Allmänna dataskyddsrättsliga regler

Dataskyddsdirektivet

I dataskyddsdirektivet finns regler om sekretess (artikel 16) och säkerhet (artikel 17) vid behandling av personuppgifter.

I artikel 16 föreskrivs att den som utför arbete under den registeransvarige (personuppgiftsansvarige) eller registerföraren (personuppgiftsbiträdet), liksom registerföraren själv, och som får tillgång till personuppgifter, får behandla dem endast enligt instruktion från den registeransvarige, om han inte är skyldig att göra det enligt lag.

Genom artikel 17.1 åläggs medlemsstaterna att föreskriva att den registeransvarige ska genomföra lämpliga tekniska och organisa-

toriska åtgärder för att skydda personuppgifter från förstöring genom olyckshändelse eller otillåtna handlingar eller förlust genom olyckshändelse samt mot ändringar, otillåten spridning av eller otillåten tillgång till uppgifterna, särskilt om behandlingen innefattar överföring av uppgifter i ett nätverk, och mot varje annat slag av otillåten behandling. Dessa åtgärder ska ”med beaktande av den nuvarande tekniska nivån och de kostnader som är förenade med åtgärdernas genomförande” åstadkomma en lämplig säkerhetsnivå i förhållande till de risker som är förknippade med behandlingen och arten av de uppgifter som ska skyddas.

Enligt artikel 17.2 ska medlemsstaterna föreskriva att den registeransvarige, som anlitar registerförare för att utföra behandling för dennes räkning, ska dels välja en registerförare som kan ge tillräckliga garantier vad gäller de tekniska säkerhetsåtgärder och de organisatoriska åtgärder som måste vidtas, dels se till att dessa åtgärder genomförs.

Som har framgått av avsnitt 10.1.2 uppställs också krav på att det träffas en bindande överenskommelse (artikel 17.3).

Dataskyddsdirektivet innehåller inga regler om möjligheter att föreskriva om undantag från bestämmelserna i artiklarna 16 och 17.

Personuppgiftslagen

Artikel 16 och 17 i dataskyddsdirektivet har införlivats i Sverige genom 30 och 31 §§ PuL under rubriken Säkerheten vid behandling. Dessa bestämmelser är avsedda att ha samma innebörd som de nämnda artiklarna (prop. 1997/98:44 s. 136). Både 30 och 31 §§ gäller utan undantag vid all slags behandling som omfattas av personuppgiftslagens tillämpningsområde. Varken 30 eller 31 § finns således med i uppräkningen i den s.k. missbruksregeln av sådana bestämmelser i personuppgiftslagen som inte behöver tillämpas vid behandling av personuppgifter i s.k. ostrukturerat material (5 a § PuL).

Enligt 30 § första stycket får den eller de personer som arbetar under biträdets eller den personuppgiftsansvariges ledning behandla personuppgifter bara i enlighet med instruktioner från den personuppgiftsansvarige. Varken av personuppgiftslagen eller av direktivet framgår emellertid hur utförliga instruktioner den personuppgifts-

ansvarige måste lämna sina medhjälpare. Datalagskommittén framhöll att den personuppgiftsansvarige i princip bär ansvaret för att instruktionerna är så tydliga att otillåten behandling inte kommer att utföras (SOU 1997:39 s. 408).

Om det i lag eller annan författning finns särskilda bestämmelser om behandling av personuppgifter i det allmännas verksamhet, ska dessa gälla i stället för den personuppgiftsansvariges instruktioner (30 § tredje stycket PuL). Enligt personuppgiftslagens förarbeten avses särskilt bestämmelser om tystnadsplikt och sekretess (prop. 1997/98:44 s. 136).

Enligt 31 § första stycket ska den personuppgiftsansvarige vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna ska åstadkomma en säkerhetsnivå som är lämplig med beaktande av de tekniska möjligheter som finns, vad det skulle kosta att genomföra åtgärderna, de särskilda risker som finns med behandlingen av personuppgifterna och hur pass känsliga de behandlade personuppgifterna är. I förarbetena sägs att paragrafen ska ha samma innebörd som artikel 17.1 och 17.2 i dataskyddsdirektivet (prop. 1997/98:44 s. 136).

Vi har i avsnitt 10.1.1. redan behandlat kravet enligt 30 § andra stycket PuL på skriftligt avtal om ett personuppgiftsbiträdes behandling av personuppgifter för den personuppgiftsansvariges räkning samt kravet i 31 § andra stycket på säkerhetsåtgärder hos personuppgiftsbiträdet m.m.

Enligt 50 § PuL får regeringen eller den myndighet som regeringen bestämmer meddela närmare föreskrifter om vilka krav som ställs på den personuppgiftsansvarige vid behandling av personuppgifter. Regeringen har i 16 § PuF bemyndigat Datainspektionen att meddela sådana föreskrifter. Hittills har det inte meddelats några föreskrifter rörande säkerhetsfrågor. Däremot har Datainspektionen publicerat allmänna råd om säkerhet för personuppgifter.

Förslaget till uppgiftsskyddsförordning

Kommissionen

I förslaget till en allmän uppgiftsskyddsförordning finns ett flertal nyheter i förhållande till dataskyddsdirektivet som har relevans för kraven på säkerhet vid personuppgiftsbehandling. De mera centrala nyheterna redovisas i det följande.

I artikel 22 beskrivs detaljerat den registeransvariges ansvar för att följa förordningen bl.a. genom att anta interna policyer och åtgärder för att säkerställa att behandling utförs i enlighet med förordningen. I det ingår att förordningens krav på åtgärder för datasäkerhet ska genomföras. Kontroll av hur verkningsfulla åtgärderna är ska också göras.

I artikel 23 fastställs den registeransvariges skyldigheter som följer av principerna om inbyggt uppgiftsskydd (data protection by design) och uppgiftsskydd som standard (data protection by default). Bland annat föreskrivs att de tekniska och organisatoriska åtgärderna ska vidtas både vid tidpunkten för fastställandet av behandlingsmetoden och vid tidpunkten för själva behandlingen. Det ska finnas rutiner som säkerställer att personuppgifter i standardfallet inte görs tillgängliga för ett obegränsat antal enskilda.

När det gäller avtal med registerförare krävs enligt artikel 26 att avtalet, utöver vad som redan följer av dataskyddsdirektivet, ska innehålla föreskrifter om att registerföraren bara får anställa personal som har åtagit sig att iaktta sekretess eller som omfattas av lagstadgad sekretessförpliktelse. Vidare får registerföraren engagera en annan registerförare bara om den registeransvarige först har godkänt det.

Genom artikel 30 åläggs den registeransvarige och registerföraren att vidta lämpliga åtgärder för säkerheten vid behandling. Bestämmelserna motsvarar i princip artikel 17.1 och 2 i dataskyddsdirektivet. En nyhet i förhållande till direktivet är att även registerföraren får en direkt skyldighet att vidta åtgärder. Vidare anges att den registeransvarige och registerföraren först ska göra en bedömning av riskerna varefter säkerhetsåtgärder ska vidtas för att skydda personuppgifterna. Kommissionen föreslås få befogenhet att anta delegerade akter enligt artikel 86 i syfte att närmare precisera kriterierna och villkoren för de tekniska och organisatoriska åtgärder som avses i artikel 30, för specifika sektorer och i specifika situa-

tioner vid behandlingen av personuppgifter, med särskild hänsyn till den tekniska utvecklingen och utvecklingen i fråga om lösningar för inbyggt integritetsskydd och uppgiftsskydd som standard. När så är nödvändigt får kommissionen även anta genomförandeakter för att specificera kraven för olika situationer.

Enligt artikel 31 ska den personuppgiftsansvarige vara skyldig att utan dröjsmål anmäla ett inträffat ”personuppgiftsbrott” till tillsynsmyndigheten. Även berörda registrerade ska, under vissa förutsättningar, informeras om ett inträffat sådant brott, se artikel 32. Med personuppgiftsbrott avses ett säkerhetsbrott som leder till förstöring, förlust eller ändringar genom olyckshändelse eller otillåtna handlingar eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på något annat sätt behandlats (artikel 4.9).

Europaparlamentet

I Europaparlamentets resolution med förslag till ändringar i förordningen föreslås ett tillägg i artikel 5 (Principer av behandling av personuppgifter) om att personuppgifter ska behandlas på ett sätt som medför ett skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse med hjälp av lämpliga tekniska eller organisatoriska åtgärder (integritet).

Beträffande artikel 23 om inbyggt uppgiftsskydd och uppgiftsskydd som standard föreslås bl.a. att hela livscykeln i hanteringen av personuppgifter ska beaktas – från insamling och behandling till radering – med systematisk inriktning på omfattande rättssäkerhetsgarantier för korrekthet, konfidentialitet, integritet, fysisk säkerhet och radering av personuppgifter. Om den registeransvarige har utfört en konsekvensbedömning avseende uppgiftsskydd enligt artikel 33, ska resultaten av bedömningen beaktas i utarbetandet av skyddet (se avsnitt 16.1 angående artikel 33).

I fråga om artikel 30 – säkerhet i samband med behandling av personuppgifter – föreslås ett flertal tillägg som bl.a. innebär närmare preciseringar av säkerhetsåtgärder som ska vidtas i olika fall.

För de artiklar som berörts ovan har parlamentet förordat – i likhet med motsvarande ställningstagande på andra områden – att de

bestämmelser som ger kommissionen befogenheter att anta delegerade akter eller genomförandeakter ska utgå.

Några kommentarer

Den föreslagna uppgiftsskyddsförordningen innehåller som synes ett flertal krav som innebär både nyheter och förtydliganden i förhållande till vad som gäller enligt dataskyddsdirektivet och personuppgiftslagen. I dataskyddsdirektivet är bestämmelserna om sekretess och säkerhet samlade i två artiklar, 16 och 17, som är mycket allmänt hållna vad avser vilken slags inriktning på tekniska eller organisatoriska åtgärder som behövs för att uppnå en lämplig säkerhetsnivå. I förordningen finns bestämmelser av betydelse för säkerheten uppdelade på ett större antal artiklar och de berör fler aspekter på skyddsbehovet än direktivet.

De föreslagna bestämmelserna torde delvis innebära klargöranden av vad som i dag redan anses följa av direktivet men innebär trots allt en betydande ökning av mängden preciserade och ovillkorliga krav på säkerhetsåtgärder jämfört med vad som följer av direktivet.

Regleringen i förordningen ställer också mycket tydliga krav på förberedande analyser, åtgärder och överenskommelser samt dokumentation över detta jämfört med vad som gäller i dag.

En av de mera grundläggande skillnaderna i förhållande till direktivet är det medansvar för skyddet av personuppgifterna som läggs på ett personuppgiftsbiträde. I sammanhanget kan nämnas att personuppgiftsbiträdets ansvar föreslås vara skadeståndssanktionerat till skillnad från vad som gäller enligt direktivet och personuppgiftslagen (artikel 77 i förordningen).

10.2.2 Innebörden av kraven på säkerhetsåtgärder m.m. vid personuppgiftsbehandling

Personuppgiftslagen innehåller alltså inga föreskrifter om vilka konkreta säkerhetsåtgärder som ska eller bör vidtas utan lagen ger en kortfattad och allmänt hållen uppräkning av de faktorer som ska beaktas av den personuppgiftsansvarige när en lämplig säkerhetsnivå ska utformas. Vid tolkningen av vad för slags åtgärder som

krävs ger dock punkten 46 i ingressen till dataskyddsdirektivet viss vägledning. I denna punkt anges att skyddet för de registrerades fri- och rättigheter förutsätter såvitt avser behandling av personuppgifter att lämpliga tekniska och organisatoriska åtgärder vidtas både när systemet för behandlingen utformas och när själva behandlingen sker, särskilt för att garantera säkerheten och för att på så sätt hindra all otillåten behandling. Det måste alltså finnas säkerhetsåtgärder som är förebyggande. Det räcker inte att den personuppgiftsansvarige vidtar reaktiva åtgärder för att ingripa mot pågående behandling som inte uppfyller personuppgiftslagens säkerhetskrav.

I förarbetena till personuppgiftslagen framhöll regeringen att de allmänt hållna reglerna på ett kortfattat och bra sätt beskriver de överväganden som måste göras i fråga om säkerhetsåtgärder. Samtidigt konstaterades att reglerna som regel inte ger tillräcklig vägledning för den personuppgiftsansvarige för att avgöra vilka säkerhetsåtgärder som bör vidtas i det enskilda fallet för att nå upp till en lämplig säkerhetsnivå och att avsikten därför var att regeringen eller den myndighet som regeringen bestämmer skulle meddela de närmare föreskrifter om säkerhetsåtgärder som behövs (prop. 1997/98:40 s. 92). Som framgått har några sådana föreskrifter dock inte meddelats. Datainspektionen har i stället valt att ge närmare vägledning genom allmänna råd. Datainspektionens beslut i tillsynsärenden som rör säkerhetsfrågor har också betydelse som vägledning för vilka specifika åtgärder som kan krävas i likartade fall.

Datainspektionens allmänna råd Säkerhet för personuppgifter, som reviderades i november 2008, riktar sig till alla som behandlar personuppgifter enligt personuppgiftslagen, alltså inte bara till myndigheter. I de allmänna råden ges exempel på administrativa och tekniska säkerhetsåtgärder som kan vidtas.

Till en början rekommenderas att verksamheter har en säkerhetspolicy, i vart fall om man hanterar personuppgifter som är känsliga eller avser en omfattande mängd. Policyn bör följas upp med kontroller av hur den följs. Arbetsrutiner m.m. i verksamheten bör utformas på sätt som underlättar att policyn följs av personalen. Vidare rekommenderas att det görs risk- och sårbarhetsanalyser för att bl.a. klarlägga vilken säkerhetsnivå som bör gälla för personuppgifterna och informationssystemen. Utbildning av perso-

nalen i säkerhetsfrågor och information om vikten av att följa konkreta säkerhetsrutiner lyfts också fram.

När det gäller råd om mer konkreta säkerhetsåtgärder som kan behövas anges bl.a. fysisk säkerhet i fråga om it-utrustningen och rutiner för säkerhetskopiering av personuppgifterna. Vidare rekommenderas system för tilldelning och kontroll av behörigheter för att förhindra obehörig användning eller åtkomst och för att kunna kontrollera användningen så att endast de som behöver uppgifter för sitt arbete får tillgång till åtkomstskyddade personuppgifter. Behandlingshistorik kan behövas i vissa fall beroende på känsligheten i personuppgifterna. När det gäller kommunikation och överföring av personuppgifter via nät måste åtgärder vidtas för att skydda uppgifterna från obehörig åtkomst eller från att förstöras eller förvanskas. Ett sätt att göra detta är att uppgifterna krypteras.

I inspektionens sammanfattning av de allmänna råden anges att den personuppgiftsansvariga bör tänka på följande åtgärder.

- Kartlägga hotbilden
- Sätta mätbara mål för säkerheten
- Fastställa policy för säkerheten
- Skapa en fungerande organisation för säkerheten
- Skaffa den utrustning som behövs och använda den rätt
- Upprätta regler och rutiner
- Informera och utbilda kontinuerligt
- Följa upp att regler och rutiner efterlevs och respekteras
- Testa säkerheten regelbundet

Underförstått ligger i de allmänna råden att de rekommenderade åtgärderna inte bara syftar till att åstadkomma ett skydd för personuppgifterna externt, dvs. utanför den egna organisationen, utan även inom denna.

10.2.3 Reglering i registerförfattningar

I en stor mängd registerförfattningar saknas särskilda regler om säkerhet och internt integritetsskydd. I allmänhet gäller därför personuppgiftslagens bestämmelser, antingen genom att det särskilt angetts att 30–32 §§ PuL ska vara tillämpliga även vid personuppgiftsbehandling enligt registerförfattningen i fråga eller därför att dessa bestämmelser ändå gäller när det handlar om en registerförfattning som enbart kompletterar personuppgiftslagen med de särbestämmelser som ansetts behövas.

Det får antas att ett skäl till avsaknaden av särreglering torde vara att det normalt inte lämpar sig att i författning slå fast vilka tekniska och organisatoriska säkerhetsåtgärder m.m. som krävs för en god informationssäkerhet och internt integritetsskydd. Den tekniska utvecklingen och övriga föränderliga förhållanden m.m. medför krav på stor flexibilitet och en detaljeringsnivå som innebär klart begränsade möjligheter att på ett över tid hållbart sätt författningsreglera frågor av det slaget.

Emellertid förekommer det i en del registerförfattningar bestämmelser som i vissa hänseenden preciserar de allmänna kraven i personuppgiftslagen på att vidta lämpliga säkerhetsåtgärder till skydd för de personuppgifter som behandlas. Det handlar då främst om regler som syftar till att motverka sådana risker för otillbörliga integritetsintrång som kan bli konsekvensen av att stora mängder eller särskilt integritetskänsliga personuppgifter blir tillgängliga för många anställda som hanterar personuppgifter i sin dagliga verksamhet inom en myndighet. Särskilda krav på behörighetsstyrning, spårbarhet och efterhandskontroll har t.ex. i detta syfte införts i vissa fall.

Ett exempel på en bestämmelse som syftar till att begränsa tillgängligheten till personuppgifter är 2 kap. 11 § polisdatalagen (2010:361) där det föreskrivs att tillgången ska begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter. Bestämmelsen kompletteras med närmare föreskrifter i 3 och 4 §§ polisdataförordningen (2010:1155) om att det vid tilldelning av behörighet för åtkomst till personuppgifter särskilt ska beaktas att det utöver tjänstemannens arbetsrelaterade behov dessutom ställs krav på utbildning och erfarenhet. Vidare ges Polismyndigheten och Säkerhetspolisen ett ansvar för att ha rutiner

inom den egna myndigheten för tilldelning, förändring, borttagning och regelbunden uppföljning av behörigheter. Det ställs således krav på en aktiv behörighetsstyrning som är flexibel och anpassningsbar till den tekniska tillgång till personuppgifter som olika tjänstemän eller personalkategorier har behov av i sin aktuella befattning.

Det förekommer inte bara bestämmelser om att behörighetstilldelningen ska styras utan också krav på att den faktiska tillgången och användningen ska kontrolleras. Ett exempel är 4 kap. 3 § patientdatalagen som ålägger den personuppgiftsansvarige att dokumentera den interna åtkomsten i behandlingshistorik för att möjliggöra efterhandskontroll. Dessutom åläggs den personuppgiftsansvarige att göra systematiska och återkommande kontroller av om någon obehörig kommit åt patientuppgifter. Samma krav gäller vid direktåtkomst till uppgifter vid sammanhållen journalföring över vårdgivargränser, 6 kap. 7 § patientdatalagen. Deltagande vårdgivare ansvarar var för sig för behörighetstilldelning och åtkomstkontroll avseende sin personal (prop. 2007/08:126 s. 148 f.). Enligt en särskild bestämmelse som riktar sig till var och en som arbetar inom hälso- och sjukvården får han eller hon ta del av dokumenterade patientuppgifter bara om han eller hon deltar i vården av patienten eller av annat skäl behöver uppgifterna för sitt arbete inom hälso- och sjukvården, 4 kap. 1 § patientdatalagen. Bestämmelsen är straffsanktionerad genom 4 kap. 9 c § BrB om dataintrång.

När en myndighet har personuppgiftsansvaret även för andras användning av ett register förekommer det att den personuppgiftsansvariga myndigheten bemyndigas meddela föreskrifter i frågor som rör informationssäkerhet. Av exempelvis 9 § lagen (2009:619) om djurskyddskontrollregister följer att Jordbruksverket kan meddela föreskrifter rörande krav på säkerhetsåtgärder som ska gälla vid t.ex. länsstyrelsers direktåtkomst till registret.

Det förekommer även bestämmelser som villkorar ett utlämnande via direktåtkomst genom krav på att den utlämnande myndigheten först försäkrar sig om att handläggare hos den mottagande myndigheten bara kan ta del av uppgifter om personer som är aktuella i ärenden hos myndigheten, se t.ex. 114 kap. 22 och 23 §§ SFB och 13 § studiestödsdataförordningen (2009:321).

10.2.4 Informationssäkerhet i ett vidare perspektiv

Myndigheters personuppgiftsansvar och det däri ingående ansvaret för att se till att lämpliga tekniska och organisatoriska säkerhetsåtgärder vidtas har ett nära samband med ansvaret för informationssäkerheten i verksamheten. Det handlar då inte bara om att skydda enskilda registrerades personliga integritet utan också om samhällets behov av att myndigheterna upprätthåller en god informationssäkerhet i sin verksamhet. All offentlig verksamhet är beroende av robusta och fungerande informationssystem samt skydd för informationen. Detta gäller såväl vid normala förhållanden som vid olika slags kriser eller extraordinära belastningar. Behovet av informationssäkerhet omfattar givetvis inte bara personuppgifter utan all slags information. Skyddsintressena är också andra än det rent persondataskyddsrättsliga. Det kan bl.a. handla om att motverka störningar i verksamheternas bedrivande, att garantera den långsiktiga offentlighetsinsynen i allmänna handlingar, att skydda rikets säkerhet m.m.

Vad avses med informationssäkerhet?

Informationssäkerhet är ett brett begrepp som enligt terminologin från Swedish Standard Institute (SIS handbok 550 utgåva 3) avser säkerhet för informationstillgångar avseende förmågan att upprätthålla önskad konfidentialitet, riktighet och tillgänglighet.

- Konfidentialitet syftar på att endast behöriga personer får tillgång till information.
- Riktighet avser att informationen inte obehörigt förstörs eller manipuleras.
- Med tillgänglighet avses att det ska finnas tillgång till informationen när den behövs.

Säkerhetsskydd och informationssäkerhet

För sekretesskyddade uppgifter som rör rikets säkerhet finns särskilda bestämmelser om informationssäkerhet i säkerhetsskyddslagen (1996:627). Med informationssäkerhet avses säkerhetsskydd

som förebygger att uppgifter av det nämnda slaget obehörigen röjs, ändras eller förstörs (7 §). Vidare föreskrivs att vid utformningen av informationssäkerheten ska behovet av skydd vid automatisk informationsbehandling beaktas särskilt (9 §).

Säkerhetsskyddslagstiftningen är för närvarande föremål för översyn. Utredningen om säkerhetsskyddslagen har nyligen lämnat förslag till en ny säkerhetsskyddslag (SOU 2015:25). I den föreslagna lagen uttrycks en bredare ansats i jämförelse med den nuvarande lagen, bl.a. i det att tillgänglighets- och riktighetsaspekterna av information och it-system lyfts fram. På så sätt vidgas tillämpningsområdet för säkerhetsskyddet till att ge skydd för informationstillgångar i samhällsviktig verksamhet som inte behöver skydd från ett konfidentialitetsperspektiv. Den föreslagna lagen avses svara mot de förändrade krav på säkerhetsskydd som bl.a. följer av utvecklingen på informationsteknikområdet, en ökad internationell samverkan och en ökad sårbarhet i samhällsviktiga funktioner.

Övergripande arbete med samhällets informationssäkerhet

Myndigheten för samhällsskydd och beredskap, MSB, har bl.a. till uppgift att stödja och samordna arbetet med samhällets informationssäkerhet samt analysera och bedöma omvärldsutvecklingen inom området. I detta ingår att lämna råd och stöd i fråga om förebyggande arbete till andra statliga myndigheter, kommuner och landsting samt företag och organisationer (11 a § förordningen [2008:1002] med instruktion för Myndigheten för samhällsskydd och beredskap). Myndigheten samverkar också med andra myndigheter med särskilda uppgifter inom informationssäkerhetsområdet, bl.a. i Samverkansgruppen för informationssäkerhet, SAMFI, vari ingår, utöver Myndigheten för samhällsskydd och beredskap, Post- och telestyrelsen, Försvarets radioanstalt, Polismyndigheten, Säkerhetspolisen, Försvarets materielverk med Sveriges Certifieringsorgan för IT-säkerhet samt Försvarsmakten med den Militära underrättelse- och säkerhetstjänsten. Nämnas kan även det informationssäkerhetsråd som finns hos Myndigheten för samhällsskydd och beredskap vari ingår företrädare för såväl myndigheter som närings-

livet. Visst samarbete sker också med Datainspektionen och Riksarkivet.

Arbetet hos Myndigheten för samhällsskydd och beredskap handlar till stor del om att stödja förebyggande åtgärder och främja ett systematiskt och långsiktigt arbete med informationssäkerhet på alla nivåer i samhället. Så sker bl.a. genom olika slags metodstöd till myndigheter eller enskilda aktörer. Myndigheten har också utformat en strategi för samhällets informationssäkerhet 2010–2015.

Varje myndighet har ett eget ansvar för informationssäkerheten i sin verksamhet vid sidan av de krav på säkerhet som gäller enligt personuppgiftslagen, arkivlagen m.m. Detta ansvar är ett uttryck för den ansvarsprincip som är grunden för samhällets krisberedskap. Ansvarsprincipen innebär att den som har ansvar för en verksamhet under normala förhållanden också har det under allvarliga händelser, kriser eller krig. I ansvarsprincipen ingår även att samverka och samordna sig med andra aktörer i den omfattning som krävs för att effektivt förebygga och hantera en allvarlig händelse (prop. 2007/08:92 s. 37 f.). I förordningen (2006:942) om krisberedskap och förhöjd beredskap – som syftar till att statliga myndigheter genom sin verksamhet ska minska sårbarheten i samhället och utveckla en god förmåga att hantera sina uppgifter under fredstida krissituationer och höjd beredskap – föreskrivs att varje myndighet ska göra en årlig risk- och sårbarhetsanalys av om det finns sådan sårbarhet eller sådana hot och risker inom myndighetens ansvarsområde som synnerligen allvarligt kan försämra förmågan till verksamhet inom området. Syftet är att stärka egen och samhällets krisberedskap (9 §). Vidare föreskrivs, under rubriken Informationssäkerhet, att varje myndighet ansvarar för att egna informationshanteringssystem uppfyller sådana grundläggande och särskilda säkerhetskrav att myndighetens verksamhet kan utföras på ett tillfredsställande sätt. Därvid ska behovet av säkra ledningssystem särskilt beaktas (30 a §).

Myndigheten för samhällsskydd och beredskap har meddelat kompletterande föreskrifter till de nyss nämnda bestämmelserna, dels MSBFS 2015:3 avseende statliga myndigheters risk- och sårbarhetsanalyser, dels MSBFS 2009:10 avseende statliga myndigheters informationssäkerhet.

Av MSBFS 2015:3 framgår bl.a. att myndighetens rutiner för att identifiera och hantera kritiska beroenden till system och tjänster

för informationshantering, som är av central betydelse för myndighetens verksamhet, är av betydelse som indikator på myndighetens krishanteringsförmåga. Delvis motsvarande bestämmelser för landsting och kommuner finns för övrigt i myndighetens föreskrifter om sådana risk- och sårbarhetsanalyser som avses i lagen (2006:544) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap (MSBFS 2015:4 och 2015:5).

Enligt MSBFS 2009:10 åligger det statliga myndigheter att i sitt arbete med informationssäkerhet tillämpa ett ledningssystem för informationssäkerhet. Det innebär att myndigheten ska

- upprätta en informationssäkerhetspolicy,
- utse personal som leder och samordnar arbetet med informationssäkerhet,
- klassificera myndighetens information med utgångspunkt i kraven på konfidentialitet, riktighet och tillgänglighet,
- utifrån risk- och sårbarhetsanalyser och inträffade incidenter bedöma hur risker ska hanteras och
- dokumentera arbetet.

Myndighetens ledning ska vidare löpande informera sig om arbetet med informationssäkerhet och minst en gång om året följa upp och utvärdera arbetet. Varje statlig myndighet ska därvid införa ett ledningssystem för informationssäkerhet (LIS) för att myndighetsledningen ska kunna styra så att rätt administrativa och tekniska säkerhetsåtgärder ska vidtas utifrån den riskbedömning ledningen gör. Standarderna för ledningssystem för informationssäkerhet, dvs. SS-ISO/IEC 27001:2006 (LIS, krav) och SS-ISO/IEC 27002:2005 (riktlinjer) utgör stöd för arbetet.

I de till MSBFS 2009:10 kompletterande allmänna råden anges bl.a. att en organisations sammantagna informationssäkerhet skapas genom en kombination av tekniska och administrativa säkerhetsåtgärder där utgångspunkten för arbetet är att risk- och sårbarhetsanalyser genomförs för att klarlägga den säkerhetsnivå som bör gälla till skydd för myndighetens organisation. Vidare lämnas bl.a. rekommendationer i fråga om att det bör upprättas riktlinjer för åtkomst- och behörighetsstyrning som en del av regelverket för infor-

mationssäkerhet. Dessa riktlinjer bör även innefatta krav på loggning och uppföljning.

I slutet av år 2013 tillsattes en utredning om strategi och mål för hantering och överföring av information i elektroniska kommunikationsnät och it-system, NISU 2014. Utredningen har bl.a. föreslagit en strategi för informations- och cybersäkerhet i staten. Ett av strategins mål är att stärka styrning och tillsyn inom området. Det ska bl.a. ske genom en nationell styrmodell för ett systematiskt informationssäkerhetsarbete i statlig verksamhet samt genom inrättandet av ett statligt myndighetsråd för informationssäkerhet bestående av företrädare för relevanta myndigheter på området. Vidare föreslås en förordning för statliga myndigheters informationssäkerhet enligt vilken Myndigheten för samhällsskydd och beredskap ska utöva tillsyn över myndigheternas informationssäkerhetsarbete (SOU 2015:23).

God offentlighetsstruktur, arkivvård m.m. och informationssäkerhet

I 4 kap. 1 § OSL finns regler om hanteringen av allmänna handlingar. Där föreskrivs bl.a. att en myndighet ska ta hänsyn till rätten att ta del av allmänna handlingar när den organiserar hanteringen av sådana handlingar. Myndigheten ska särskilt se till att allmänna handlingar kan skiljas från andra handlingar och lämnas ut med den skyndsamhet som krävs enligt tryckfrihetsförordningen. Myndigheter ska också se till att rätten att ta del av allmänna handlingar enligt tryckfrihetsförordningen säkerställs samtidigt som sekretesskyddet upprätthålls. Handlingar med olika offentlighetsstatus ska alltså kunna hållas i sär. Av offentlighets- och sekretesslagen följer även indirekt ett krav på att uppgifter hos myndigheterna skyddas informationssäkerhetsmässigt, i synnerhet vad gäller uppgifter som är sekretessreglerade.

Det sistnämnda kan illustreras med ett JO-beslut med anledning av en anmälan om att en kommunal nämnd hade röjt en persons sekretesskyddade namn vid handläggning av ett ärende om försörjningsstöd. Röjandet orsakades av att handläggarna använde ett elektroniskt verksamhetssystem där det inte tydligt framgick om det fanns någon sekretessmarkering för den enskildes personuppgifter. JO uttalade att det är mycket allvarligt att en myndighet som i sitt

dagliga arbete hanterar en mängd personuppgifter som omfattas av sekretess inte har ett verksamhetssystem som i det hänseendet är säkert (beslut 2014-02-05, dnr 5932-2012). Såsom exemplet visar sammanfaller i praktiken kravet på sekretesskydd ofta med flera av de krav på säkerhetsåtgärder som persondataskyddsregleringen uppställer. Detsamma kan sägas gälla beträffande de krav som arkivvården ställer.

I arkivlagen finns närmare bestämmelser om säkerhetsåtgärder i olika avseenden. Enligt 6 § 3 arkivlagen ingår det i varje myndighets ansvar för arkivvården att skydda sitt arkiv mot förstöring, skada, tillgrepp och obehörig åtkomst. Detta ansvar avser skydd mot yttre och inre faktorer som kan skada arkivet, t.ex. tekniska problem i ett it-system för arkivering som förstör eller försvårar åtkomst till handlingar i systemet. I en elektronisk miljö innebär det vidare att det måste finnas skydd mot dataintrång. Att arkivet ska skyddas mot obehörig åtkomst syftar i första hand på att sekretesskyddet för uppgifter i handlingarna ska kunna upprätthållas. Handlingar som kan innehålla uppgifter som omfattas av sekretess måste således hanteras så att inte obehöriga kan läsa dem (Ulrika Geijer m.fl., Arkivlagen. En kommentar, uppl. 1:1, 2013, s. 174).

De krav på informationssäkerhetsåtgärder som följer av arkivlagens bestämmelser om arkivvård är alltså i vissa avseenden desamma som de som följer av personuppgiftslagens krav på säkerhetsåtgärder till skydd för personuppgifter som behandlas (31 § PuL). Det övergripande syftet med arkivvården är emellertid inte att skydda människor mot kränkningar av deras personliga integritet utan att tillgodose rätten att ta del av allmänna handlingar, behovet av information för rättskipningen och förvaltningen samt forskningens behov (3 § tredje stycket arkivlagen).

Riksarkivet har rätt att meddela föreskrifter för statliga myndigheters arkiv om skydd av arkivet med stöd av 11 § 2 arkivförordningen (1991:446). Sådana föreskrifter gäller dock inte för riksdagens myndigheter, regeringen, Regeringskansliet eller utrikesrepresentationen (10 § första stycket arkivförordningen).

I 6 kap. Riksarkivets föreskrifter och allmänna råd om elektroniska handlingar (upptagningar för automatiserad behandling) – RA-FS 2009:1 – har Riksarkivet meddelat föreskrifter om informationssäkerhet. Där föreskrivs bl.a. att en myndighet ska, för att säkerställa ett bevarande av de elektroniska handlingarna, skapa och upp-

rätthålla rutiner samt vidta åtgärder för att skydda handlingarna från skada, manipulation, obehörig åtkomst och stöld. Det kan vidare nämnas att föreskrifterna anger samma standarder för informationssäkerhet som anges av Myndigheten för samhällsskydd och beredskap (MSBSF 2009:10), dvs. SS-ISO/IEC 27001:2006 (LIS) och SS-ISO/IEC 27002:2005.

Vidare ska myndigheten upprätta en informationssäkerhetsplan, dvs. en plan för hur de elektroniska handlingarna ska skyddas. Planens efterlevnad ska regelbundet kontrolleras och dokumenteras (2 §). Det åligger myndigheten att också genomföra en riskanalys innan driftsättning sker eller innan uppdrag ges till annan myndighet eller enskild för att bedöma behovet av säkerhetsrutiner (3 §). Elektroniska handlingar ska förses med behörighetssystem, loggsystem och skydd mot skadlig kod om det inte är uppenbart obehövligt (4 §). Säkerhetskopior ska regelbundet framställas och särskilda krav gäller avseende rutinerna för detta och för övrig hantering av säkerhetskopiorna (5 och 6 §§). Elektroniska handlingar ska hanteras och transporteras under sådana former att de inte skadas och så att de inte riskerar att bli utsatta för obehörig åtkomst. Handlingarna och dokumentationen om dessa ska transporteras åtskilda. Särskild aktsamhet ska iakttas när det gäller handlingar som kan omfattas av sekretess (8 §).

Riksarkivet är tillsynsmyndighet för statliga myndigheter och gör regelbundna inspektioner av att myndigheterna fullgör sina skyldigheter enligt arkivlagstiftningen.

10.2.5 Våra överväganden och förslag

Allmänna krav på säkerhetsåtgärder m.m.

Förslag: Skyldigheterna i fråga om säkerhetsåtgärder och lämplig säkerhetsnivå ska framgå genom en bestämmelse i lagen som ersätter 31 § första stycket PuL. Där ska det föreskrivas att personuppgiftsansvariga myndigheter är skyldiga att vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas och att åtgärderna ska åstadkomma en lämplig säkerhetsnivå som ska bestämmas utifrån de risker som behandlingen medför och personuppgifternas karaktär. Vidare

ska framgå att säkerhetsarbetet ska omfatta förebyggande, löpande och uppföljande åtgärder samt att säkerhetsarbetet ska ske med beaktande av andra föreskrifter om informationssäkerhet i lag eller annan författning. Härmed klargörs den nära kopplingen mellan den persondataskyddsrättsliga regleringen av säkerheten för personuppgifter och det vidare regelverk om informationssäkerhetsansvar som myndigheterna också är skyldiga att följa.

Det är av central betydelse att myndigheters behandling av personuppgifter sker under former som är säkra och som innebär att uppgifterna aktivt skyddas från förstöring, obehörig åtkomst eller okontrollerad spridning m.m. Det är av betydelse inte bara för det dataskydd som måste tillkomma de enskilda registrerade utan också för att allmänhetens förtroende för myndigheternas informationshantering upprätthålls. Säkerhetsfrågor har givetvis också, i det större perspektivet, en central betydelse för att den offentliga verksamheten ska fungera på ett ändamålsenligt och tillförlitligt sätt.

Som framgått är det i allt väsentligt personuppgiftslagens bestämmelser om säkerhet vid behandling av personuppgifter som gäller för informationssäkerheten vid myndigheters behandling av personuppgifter. De särregler om säkerhet och internt integritetsskydd som förekommer i registerförfattningar är ofta ganska allmänt hållna.

Myndigheternas förutsättningar och behov i fråga om informationssäkerhet varierar i hög grad. De grundläggande krav på säkerheten vid personuppgiftsbehandling som dataskyddsdirektivet föreskriver är emellertid allmängiltiga och bör komma till uttryck i den nya lagen.

Liksom i personuppgiftslagen bör därför föreskrivas att en personuppgiftsansvarig myndighet ska vidta tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Vi bedömer att det i en samlad reglering för myndigheters behandling av personuppgifter varken är påkallat eller lämpligt att närmare precisera vad för slags risker som personuppgifter ska skyddas mot (jfr artikel 17.1). Däremot ska, liksom enligt personuppgiftslagen, framgå att säkerhetsarbetet ska åstadkomma en lämplig säkerhetsnivå i förhållande till de risker som behandlingen medför och personuppgifternas karaktär. Enligt vår bedömning är det däremot knappast motiverat att på myndighetsområdet särskilt föreskriva

att detta ska göras med beaktande av den nuvarande tekniska nivån och de kostnader som är förenade med åtgärderna. Detta är en självklarhet och det torde för övrigt följa, i vart fall indirekt, av annan reglering av myndigheternas verksamhet att sådana faktorer måste beaktas när myndigheterna gör avvägningar beträffande vad som är en lämplig säkerhetsnivå. Både för statliga och kommunala myndigheter gäller t.ex. att de ska hushålla väl med allmänna medel (3 § myndighetsförordningen och 8 kap. 1 § KL).

I förhållande till den rent persondataskyddsrättsliga regleringen ser vi emellertid ett behov av en precisering rörande hur myndigheternas säkerhetsarbete bör bedrivas. Det har i vårt arbete framkommit att det förekommer brister angående behovet av att säkerhetsarbetet sker systematiskt och inbegriper förebyggande, löpande och uppföljande åtgärder av olika slag som ser till helheten i personuppgiftsbehandlingen. Det är därför önskvärt att det tydliggörs i lagen att detta sätt att arbeta med säkerhetsfrågorna är av central betydelse för ett gott personuppgiftsskydd.

Som exempel på ett systematiskt säkerhetsarbete tillämpat på en enstaka teknisk säkerhetsåtgärd kan nämnas behandlingshistorik i form av loggning av sökningar på personuppgifter. Det räcker då inte med att planera och installera funktioner som möjliggör loggning. Loggning måste sedan också faktiskt ske liksom kontroll av att den fungerar på avsett sätt. Redan vetskapen om att loggning sker kan verka förebyggande och t.ex. motverka obefogade sökningar. Men även uppföljningen av loggningarna i efterhand måste ske systematiskt.

Vi har vidare kunnat konstatera att det förhållandet att myndigheters arbete med informationssäkerhet regleras i författningar med i huvudsak andra syften än det persondataskyddsrättsliga kan leda till tillämpningsproblem för myndigheterna. Det gäller dels att det kan uppstå konflikter mellan de olika skyddsintressen som reglerna tar sikte på, dels att ansvaret för informationssäkerhetsfrågor inte alltid är organisatoriskt samordnat inom en myndighet. I den mån fokus i säkerhetsarbetet varierar, kan det påverka de avvägningar som görs vid utformningen av olika säkerhetsåtgärder och det finns då en risk att skyddet för personuppgifter inte prioriteras på ett adekvat sätt. Några egentliga regelkonflikter mellan den dataskyddsrättsliga regleringen och den allmänna informationssäkerhetsregleringen kan vi emellertid inte se. Däremot finns anled-

ning, menar vi, att i den nya lagen tydliggöra den nära koppling som finns till andra bestämmelser om informationssäkerhet som gäller för myndigheterna och som berörts i det föregående.

De säkerhetsåtgärder som persondataskyddsregleringen kräver tar sikte på vad som behövs för skyddet av personuppgifter. Detta kan föranleda säkerhetsskyddande åtgärder som andra regelverk inte påkallar. Så kan exempelvis vara fallet när det gäller behovet av att skapa ett internt skydd för personuppgifter inom en myndighet så att t.ex. otillåten användning förhindras och att överträdelser mot t.ex. interna föreskrifter motverkas, upptäcks och beivras.

Med den informationstekniska utvecklingen och den tilltagande komplexiteten i myndigheternas informationshantering går det emellertid inte att betrakta arbetet med att skapa säkerhet vid personuppgiftsbehandling som en isolerad uppgift skild från övrigt informationssäkerhetsarbete. För att tydliggöra detta bör det i den nya lagen införas en erinran om att myndigheterna vid utformningen av säkerhetsåtgärder ska beakta bestämmelser om informationssäkerhet i annan lag eller författning som gäller för myndigheten. En sådan erinran är framför allt ägnad att samordna uppfyllandet av skyldigheterna enligt de olika regelverken men tydliggör samtidigt att regelverken gäller parallellt och inte nödvändigtvis är överlappande.

Sammanfattningsvis föreslår vi således att det ska framgå av den nya lagen att myndigheter ska vara skyldiga att vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Säkerhetsarbetet ska omfatta förebyggande, löpande och uppföljande åtgärder och ska åstadkomma en lämplig säkerhetsnivå i förhållande till de risker som behandlingen medför och till personuppgifternas karaktär. Vid utformningen av säkerhetsåtgärderna ska myndigheten även beakta bestämmelser om informationssäkerhet i annan lag eller författning som gäller för myndigheten. Det angivna bör framgå direkt av lagtexten utan hänvisning till 31 § PuL.

De behov av specifika regler i fråga om säkerhetsåtgärder som kan finnas inom vissa sektorer, hos vissa myndigheter eller verksamheter bör tillgodoses genom föreskrifter i förordning eller, efter bemyndigande, i föreskrifter som meddelas av Datainspektionen eller den myndighet som regeringen annars kan komma att bestämma.

Tillgängligheten till personuppgifter inom en myndighet

Förslag och bedömning: En bestämmelse införs som innebär en skyldighet för varje myndighet att se till att anställda och andra som arbetar hos myndigheten bara ges tillgång till personuppgifter utifrån vad som krävs för arbetsuppgifterna. Detta ska gälla i fråga om såväl personuppgifter i myndighetens egna informationssamlingar som personuppgifter som myndigheten får tillgång till genom direktåtkomst eller andra former av informationsutbyte.

Det behövs inte någon bestämmelse om att den som arbetar hos en personuppgiftsansvarig myndighet får behandla personuppgifter bara i enlighet med instruktioner från den personuppgiftsansvarige (jfr 30 § första stycket PuL). Inte heller behövs någon särskild bestämmelse om informationssäkerhet hos ett personuppgiftsbiträde utöver vad som föreslagits i avsnitt 10.1.4.

Ju fler personer inom en organisation som har tillgång till personuppgifter, desto större är riskerna för obefogad åtkomst eller spridning av uppgifterna på sätt som innebär otillbörliga intrång i de registrerades personliga integritet. Detta behöver inte handla om medvetet missbruk utan kan bero på okunskap eller rena misstag.

Utbildning i informationssäkerhets- och persondataskyddsfrågor och att all personal görs medvetna om vad som gäller för hans eller hennes användning av personuppgifter är i sig en viktig organisatorisk säkerhetsåtgärd men är normalt inte en tillräcklig åtgärd. Att tillgången till personuppgifter i så stor utsträckning som möjligt faktiskt begränsas till vad var och en behöver för att fullgöra sitt arbete är, som vi ser det, en nödvändig säkerhetsåtgärd för att skapa ett tillfredsställande internt skydd för personuppgifter vid myndigheters informationshantering. Vi menar att ett behov av behörighetsstyrning kan sägas föreligga generellt. Vi föreslår mot den bakgrunden en bestämmelse som ska gälla för alla myndigheter som omfattas av lagen och som innebär att behörighetsstyrning ska ske.

Hur behörighetssystem bör vara utformade går däremot inte att ange i generella termer. Detta måste utformas specifikt för respektive verksamhet. Generellt sett kan dock sägas att ju mer omfattande ett informationshanteringssystem är, desto större mängd olika behörighetsnivåer bör finnas. Uppgifternas karaktär spelar också

stor roll. Exempelvis bör tillgång till sekretessbelagda personuppgifter som utgångspunkt givetvis vara begränsad. Samtidigt kan förhållandena vara sådana, t.ex. vid små myndigheter, att i princip hela personalen, eller i vart fall flertalet, måste ha full tillgång för att kunna utföra sina arbetsuppgifter. Innebörden av den regel vi föreslår är att myndigheter dock alltid ska vara skyldiga att pröva anställdas och uppdragstagares behov av tillgång utifrån vad arbetsuppgifterna kräver och begränsa tillgången i enlighet med detta.

Vidare innebär bestämmelsen att vid direktåtkomst varje myndighet måste pröva sin egen personals tillgång till andra myndigheters personuppgifter. Vid direktåtkomst bör det enligt vår mening alltså normalt vara den myndighet som en person arbetar hos som ansvarar för behörighetstilldelningen snarare än den utlämnande myndigheten. Det är den mottagande myndigheten som bestämmer ändamålen för behandlingen och ansvarar för vad den egna personalen gör. En helt annan sak är att erforderliga behörighetsbegränsningar rent tekniskt givitvis kan anordnas hos den av myndigheterna där det enklast kan ske.

Den bestämmelse som vi föreslår innebär en skyldighet för myndigheten att begränsa tillgången som ett led i myndighetens personuppgiftsansvar. I ansvaret för behörighetstilldelningen ingår att se till så att den enskilde befattningshavaren får information om innebörden av behörigheten. Det behövs emellertid inte särskilda föreskrifter om detta.

Bestämmelsen innebär givetvis inget hinder mot att vid behov genom föreskrifter i förordning meddela särskilda regler om behörighetsbegränsningar.

Enligt vår bedömning behövs det inte någon föreskrift i den nya lagen motsvarande vad som anges i artikel 16 i dataskyddsdirektivet om att den som utför arbete under den registeransvarige, och som får tillgång till personuppgifter, ”får behandla dem endast enligt instruktioner från den registeransvarige, om han inte är skyldig att göra det enligt lag” (jfr 30 § PuL). Myndigheter har redan en skyldighet att instruera sina befattningshavare så att de hanterar myndighetens information på ett sätt som överensstämmer med de regler som styr myndigheternas verksamhet och informationshantering.

Risk- och sårbarhetsanalys samt överenskommelse om säkerhetsåtgärder vid direktåtkomst m.m.

Förslag: Innan en utlämnande myndighet medger direktåtkomst till personuppgifter ska myndigheten göra en risk- och sårbarhetsanalys. Vidare ska myndigheten komma överens med mottagaren av personuppgifterna hur behövligt skydd för personuppgifterna ska säkerställas. Motsvarande ska gälla vid andra former av informationsutbyten eller samarbeten som innebär behandling av personuppgifter i gemensamma eller annars integrerade informationssystem.

När personuppgifter överförs mellan myndigheter kan alltså frågor uppstå om vem som är ansvarig för att personuppgifterna skyddas under och efter överföringen. Utgångspunkten är då att ansvaret följer personuppgiftsansvaret. Som har framgått är det dock inte alltid så lätt att slå fast hur personuppgiftsansvaret avgränsas då flera myndigheter är involverade i en personuppgiftsbehandling, t.ex. vid direktåtkomst. Inte ens då personuppgiftsansvaret reglerats i en registerförfattning står det alltid helt klart vad som gäller i enskilda fall t.ex. i fråga om den utlämnande myndighetens eventuella personuppgiftsansvar för en mottagande myndighets användning av ett register vad avser frågor om när, hur och varför mottagarmyndighetens personal gör sökningar i registret.

Som vi har framhållit tidigare (se avsnitt 10.1.4) omfattar personuppgiftsansvaret övergripande frågor såsom att tillse att behandlade personuppgifter skyddas genom tekniska och organisatoriska säkerhetsåtgärder. Vi har föreslagit att det ska gälla ett krav på att en utlämnande myndighet ska vara skyldig att, innan direktåtkomst till personuppgifter medges, komma överens med mottagaren av personuppgifterna hur utövandet av personuppgiftsansvaret med avseende på de skyldigheter som följer av lagen eller föreskrifter som meddelats i anslutning till lagen ska ske och att motsvarande krav ska gälla även vid andra former av informationsutbyten eller samarbeten som innebär behandling av personuppgifter i gemensamma eller annars integrerade informationssystem.

Det är alltså av väsentlig betydelse att det alltid klarläggs hur personuppgiftsansvaret fördelar sig beträffande olika moment i ”gemensamma” behandlingar. Att detta sker är av avgörande betyd-

else inte minst i fråga om tekniska och organisatoriska säkerhetsåtgärder. Tydlighet i ansvarsförhållanden vid myndighetsövergripande samarbeten är centralt för personuppgiftsskyddet liksom för informationssäkerheten i stort. Det är av största betydelse att sådana frågor i reds ut i förväg mellan de inblandade aktörerna. Mot den bakgrunden föreslår vi att det i överenskommelsen särskilt ska anges hur skyddet för personuppgifterna ska säkerställas. Det kan också framhållas att det är viktigt att överenskommelsen följs upp även sedan direktåtkomsten etablerats. Det följer emellertid redan av det allmänna kravet som vi föreslagit ovan som innebär att säkerhetsarbetet ska ske löpande och vara uppföljande.

Vi föreslår vidare att den utlämnande myndigheten vid direktåtkomst därutöver ska göra en särskild risk- och sårbarhetsanalys innan sådan medges. Motsvarande skyldighet ska gälla för myndigheter vid annan samverkan som innebär behandling av personuppgifter i gemensamma eller annars integrerade informationssystem. Den särskilda risk- och sårbarhetsanalysen ska vara inriktad på att ge det underlag som behövs för att sedan kunna bedöma om och hur det är möjligt att åstadkomma en lämplig säkerhetsnivå genom adekvata tekniska och organisatoriska säkerhetsåtgärder.

När myndigheter lämnar ifrån sig den faktiska behandlingen och därmed i viss mån kontrollen över personuppgifterna blir frågor om säkerhet och skydd för personuppgifterna särskilt betydelsefulla. Vi har i avsnitt 10.1.4 behandlat frågor om anlitande av personuppgiftsbiträde. I det sammanhanget har vi bl.a. föreslagit att den personuppgiftsansvariga myndighetens instruktioner till biträdet ska dokumenteras i parternas avtal. Sådana instruktioner måste, som vi ser det, även innehålla avtalsvillkor gällande tekniska och organisatoriska säkerhetsåtgärder till skydd för personuppgifterna.

11 Att lämna ut personuppgifter i elektronisk form

11.1 Reglering av direktåtkomst

11.1.1 Definition av begreppet direktåtkomst

Bakgrund

Vi har ovan (se avsnitt 5.7) redovisat vår uppfattning att det alltjämt finns skäl för att rättsligt skilja på begreppen direktåtkomst och annat elektroniskt utlämnande. Vår uppfattning baseras bl.a. på den omständigheten att en viss åtskillnad mellan de olika begreppen redan har lagts fast i praxis genom att uttalanden om hur direktåtkomst bör definieras i förarbetena till 11 kap. 4 § OSL får anses ha bekräftats i rättsfallet HFD 2011 ref. 52. Av dessa uttalanden följer att en direktåtkomst är för handen när en mottagande myndighet har getts en teknisk tillgång till upptagningar hos annan myndighet så att de kan ”läsas, avlyssnas eller på annat sätt uppfattas”, varmed de anses expedierade från den utlämnande myndigheten. Därmed får de också anses förvarade hos och, som huvudregel, inkomna till den mottagande myndigheten i den mening som avses i 2 kap. 3 och 6 §§ TF.

Av rättsfallet HFD 2011 ref. 52 kan emellertid inte dras någon självklar slutsats av vad uttrycket läsas, avlyssnas eller uppfattas på annat sätt innebär för de olika former av elektroniska utlämnanden som kan sägas befinna sig i ”gråzonen” mellan direktåtkomst och annat elektroniskt utlämnande. Det finns alltså ännu ingen praxis som ger ett klart svar på i vilken mån sådana former av utlämnanden är att anse som direktåtkomst. Samtidigt innebär regleringen i 2 kap. TF att endera är det fråga om direktåtkomst i nu

angiven mening eller så är det inte det. Avgörande blir bedömningen av omständigheterna i det enskilda fallet.

Utredningen har i denna del av uppdraget inget mandat att föreslå några grundlagsändringar. Den fråga vi därför har ställt oss är om det finns skäl att, för att inte behöva avvakta en utveckling i rättspraxis, nu lämna ett förslag på en definition av begreppet direktåtkomst i vanlig lag som syftar till att klargöra vad som ska gälla i den ”gråzon” som kan uppfattas finnas för närvarande.

Våra överväganden

Bedömning: Begreppet direktåtkomst bör definieras, liksom hittills, på så sätt att en direktåtkomst föreligger om en myndighet hos en annan myndighet har en sådan teknisk tillgång till upptagningar som avses i 2 kap. 3 § andra stycket TF. Någon annan – exempelvis snävare – avgränsning i vanlig lag föreslås inte.

Bestämmelserna i 2 kap. TF samt i offentlighets- och sekretesslagen (2009:400), exempelvis 7 kap. 2 § och 8 kap. 1 §, bygger på att myndigheternas verksamheter i rättslig mening gränsar till varandra. Vid ett utbyte av uppgifter sker detta alltså över en och samma gräns och däremellan finns inget utrymme. Enkelt uttryckt innebär det att uppgifter beroende på vilken sida om gränsen de befinner sig antingen finns hos den ena eller andra myndigheten och de ingår då i den ena eller andra myndighetens verksamhet. Uppgifter kan också finnas samtidigt hos båda myndigheterna om de delar på en tillgång till uppgifterna. Uppgifterna ingår då i båda myndigheternas verksamhet. Frågan om var gränsen går mellan myndigheter som deltar i ett elektroniskt uppgiftsutbyte kan dock inte göras liktydig med att ta ställning till vilka handlingar som är att betrakta som allmänna hos de olika myndigheterna. Utgångspunkten är emellertid reglerna i 2 kap. TF, framför allt 3 §, som reglerar när en upptagning anses förvarad hos en myndighet. Om en myndighet har gjort en upptagning åtkomlig för en annan myndighet på så sätt att 2 kap. 3 § TF blir tillämplig på upptagningen är den att anse som förvarad även hos den mottagande myndigheten. En rättslig gräns mellan de båda myndigheterna har alltså passerats, dvs. det finns i rättslig mening ingen oklarhet om på vilken sida om

gränsen som upptagningen befinner sig. Det innebär dock inte med automatik att upptagningen är att betrakta som allmän handling hos den mottagande myndigheten eftersom det finns flera undantag i 2 kap. TF från när i och för sig enligt 2 kap. 6 § inkomna, och således förvarade, handlingar ska anses vara allmänna. Som exempel kan nämnas den s.k. biblioteksregeln i 2 kap. 11 § första stycket 3 TF som bl.a. innebär att information på öppna webbplatser som myndigheten har åtkomst till inte är att anse som allmänna handlingar.

Om en handling har expedierats på det sätt som avses i 2 kap. 7 § TF kan också en rättslig gräns sägas ha passerats. Om en handling i tryckfrihetsförordningens mening har expedierats från den utlämnande myndigheten och därmed gjorts tillgänglig för en annan myndighet så att 2 kap. 3 § TF är tillämplig kan det alltså slås fast att handlingen har passerat den rättsliga gränsen mellan myndigheterna. Som sagt är det en senare fråga om handlingen också ska anses vara allmän hos den mottagande myndigheten. Den frågan har emellertid ingen omedelbar betydelse för hur två myndigheter rättsligt gränsar till varandra. Exempelvis skyddas uppgifter i handlingen av sekretess enligt offentlighets- och sekretesslagen hos den mottagande myndigheten, eftersom den förvaras där, oavsett om handlingen är allmän eller inte. En myndighet är också personuppgiftsansvarig för personuppgifter i en handling som förvaras hos myndigheten oavsett om handlingen är allmän eller inte.

Ett försök att i vanlig lag skapa en annan definition av begreppet direktåtkomst än den som i dag får anses gälla och som utgår från 2 kap. 3 § TF skulle enligt vår bedömning innebära att det skapas nya och andra gränser mellan myndigheterna än de som följer av bestämmelserna i 2 kap. TF och offentlighets- och sekretesslagen. Det får till följd att det i samband med elektroniska utlämnanden bildligt talat riskerar att skapas ett utrymme mellan myndigheternas gränser. Mellanrummet uppstår om det sätts upp andra, snävare gränser än vad som enligt tryckfrihetsförordningen gäller vid utbyte av uppgifter mellan myndigheter. I detta rum finns inte några givna svar på eller hållpunkter för vilken myndighet som ansvarar för vad, exempelvis när det gäller behandling av personuppgifter eller vilket sekretesskydd som ska upprätthållas. Även den förvaltningsrättsliga ansvarsfördelningen kan bli oklar. Man kan säga att det alltså riskerar att uppstå en form av ansvarsmässigt och rättsligt

vakuum. Sådana uppgiftsutbyten som kan sägas ske i den ovan omtalade gråzonen innebär emellertid i praktiken att de inblandade myndigheterna de facto har vidtagit en rad åtgärder och även tekniskt påbörjat uppgiftsutbytet i fråga. Sådana åtgärder aktualiserar både verksamhetsansvar och personuppgiftsansvar på ömse sidor. Det kan inte anses tillfredsställande att sådana åtgärder ska få vidtas utan att det står klart inom ramen för vilken myndighets verksamhet som detta sker, i synnerhet inte när åtgärderna tar sikte på personuppgifter. Enligt vår mening får det därför anses principiellt tveksamt att skapa ett rättsligt mellanrum mellan myndigheternas gränser genom att avgränsa olika former av elektroniska utlämnanden på ett annat sätt än det som följer av 2 kap. TF och offentlighets- och sekretesslagen.

Enligt vår uppfattning kan man också fråga sig vad som finns att tjäna på att i samband med att man definierar olika elektroniska utlämnandeformer sätta upp andra gränser för myndigheters utbyte av uppgifter än vad som ändå redan gäller beträffande handlingsoffentlighet. Ett problem sammanhänger med att begreppet direktåtkomst i så fall inte torde kunna avgränsas med en tillämpning av 2 kap. 3 § andra stycket TF. Det skulle då inte vara tillräckligt att bedöma om en teknisk tillgång innebär att en upptagning kan läsas, avlyssnas eller på annat sätt uppfattas. Det måste i stället formuleras ett annat kriterium. Det torde möta stora svårigheter att formulera ett sådant nytt kriterium som blir så tydligt och lättillämpat att det innebär en förenkling i förhållande till vad som ändå gäller enligt tryckfrihetsförordningen. Man kan befara att det i stället skapas en ännu större gråzon där fler former av elektroniska utlämnanden kan komma att hamna p.g.a. att det blir ännu svårare att avgöra om de är att anse som direktåtkomst eller en annan utlämnandeform.

Det får visserligen anses i viss mån otillfredsställande att det i dag inte står helt klart vid en tillämpning av 2 kap. 3 § TF hur vissa former av elektroniska uppgiftsutbyten ska definieras, dvs. om de utgör direktåtkomst eller inte. Enligt vår uppfattning innebär ett försök att skapa en annan avgränsning emellertid inte att en större tydlighet kan uppnås, utan det riskerar tvärtom att leda till ökad otydlighet. Som redan framgått anser vi därutöver att det redan av principiella skäl är olämpligt att utforma en avgränsning vid elektroniska utlämnanden som avviker från vad som annars gäller

vid överföring av uppgifter mellan myndigheter och på så sätt skapa ett utrymme – ett slags ansvarsmässigt och rättsligt vakuum – mellan myndigheter. Till detta kommer att det finns en uppenbar risk med att söka åstadkomma en reglering i syfte att fånga upp de tekniska former av åtkomst som används i dag eftersom en sådan riskerar att inte kunna tillämpas över tid.

I syfte att uppnå ett regelverk som i så stor utsträckning som möjligt är enhetligt när det gäller myndigheters hantering av information och som håller över tid anser vi således att övervägande skäl talar för att begreppet direktåtkomst bör, liksom hittills, ta sikte på det förhållandet att en myndighet hos en annan myndighet har en sådan teknisk tillgång till upptagningar som avses i 2 kap. 3 § andra stycket TF. Enligt vår bedömning bör alltså någon annan och snävare avgränsning inte utformas. Det innebär att myndigheterna, och även lagstiftaren, på samma sätt och utifrån samma kriterier som gäller enligt 2 kap. TF får bedöma om ett planerat uppgiftsutbyte ska ske i form av direktåtkomst eller på annat sätt. Vad som gäller i fråga om de elektroniska utlämnandeformer som kan uppfattas befinna sig i en gråzon mellan direktåtkomst och annat elektroniskt utlämnande får alltså bedömas utifrån vad som kan läsas ut av framför allt 2 kap. 3 § TF och praxis i anslutning till det lagrummet. Vårt ställningstagande i denna del innebär alltså att myndigheterna på samma sätt som i dag och utifrån samma definition får bedöma om ett avsett uppgiftsutbyte utgör direktåtkomst eller en annan form av elektroniskt utlämnande.

11.1.2 Bör det finnas ett generellt krav på författningsstöd för direktåtkomst?

Innebär nuvarande bestämmelser ett krav på författningsstöd?

Vad brukar lagstiftarens utgångspunkt vara?

Av 10 kap. 28 § OSL följer att en uppgiftsskyldighet som bryter den sekretess som annars gäller mellan två myndigheter ska regleras genom en bestämmelse i lag eller förordning. I det fallet krävs alltså en uttrycklig reglering som ska införas på åtminstone förordningsnivå. När det däremot gäller direktåtkomst finns i gällande rätt

inget generellt krav på att en direktåtkomst förutsätter att det genom en föreskrift uttryckligen har tillåtits att den ska få förekomma.

Av förarbeten till bestämmelser om direktåtkomst framgår att lagstiftaren ibland emellertid tycks ha utgått från ett antagande om att det finns ett krav på att direktåtkomst uttryckligen ska tillåtas genom en föreskrift. Ett exempel på det är bestämmelserna om direktåtkomst till Skatteverkets beskattningsdatabas. I lagtexten räknas det upp vilka myndigheter som får ha direktåtkomst till beskattningsdatabasen. Det uttrycks emellertid inte att det ”endast” är dessa myndigheter som får ha direktåtkomst. Av förarbetena framgår dock att det är syftet med bestämmelserna. Där anförs nämligen att förutsättningarna för åtkomsten borde föreskrivas i lag, medan regeringen borde ha möjlighet att närmare föreskriva om vilka uppgifter åtkomsten får avse (prop. 2000/01:33 s. 133). I detta fall har bestämmelserna alltså utformats med syfte att de positivt ska ange i vilka fall direktåtkomst får medges, dvs. det är bestämmelser som syftar till att tillåta något som annars skulle vara otillåtet. Om det verkligen är så, eller om bestämmelserna ger uttryck för att man har ansett det lämpligt att just på skatteområdet anlägga detta synsätt, framgår inte av förarbetena. Exempelvis förs det inget resonemang om var det i så fall uttrycks ett krav på en positiv föreskrift som tillåter direktåtkomst. Det konstateras endast att sådana regler också tidigare har haft form av lag (a. prop. s. 133). I sammanhanget kan nämnas att Socialtjänstdatautredningen däremot gjorde ett mer klart ställningstagande i frågan. Utredningen ansåg att eftersom dess förslag till en ny lag om behandling av personuppgifter inom socialtjänsten inte innehåller några bestämmelser om direktåtkomst, innebär det att någon direktåtkomst inte får förekomma (SOU 2009:32 s. 309).

Bestämmelser om direktåtkomst på många andra myndighetsområden synes däremot utgå från ett antagande om att direktåtkomst kan vara tillåten även om det inte finns någon föreskrift som medger det. Både bestämmelserna om direktåtkomst till socialförsäkringsdatabasen och till uppgifter inom socialtjänsten har utformats med en sådan utgångspunkt. Det är i dessa fall alltså frågan om bestämmelser som inskränker möjligheterna att medge direktåtkomst, dvs. de syftar till att begränsa något som annars skulle vara tillåtet.

Följer det något krav på reglering av en direktåtkomst av personuppgiftslagen?

I personuppgiftslagen finns inga bestämmelser som uttryckligen tar sikte på direktåtkomst. Den lagen berör över huvud taget inte frågan om olika utlämnandeformer. Det kan ändå finnas anledning att överväga om någon eller några av lagens bestämmelser i vart fall indirekt ställer krav på en viss reglering i samband med direktåtkomst.

Det kan då inledningsvis konstateras att personuppgiftslagens bestämmelser alltså inte medför några uttryckliga krav på att en direktåtkomst ska ha stöd i en föreskrift för att vara tillåten. Om åtkomsten avses omfatta känsliga personuppgifter krävs emellertid författningsstöd. En behandling av känsliga personuppgifter förutsätter ju att det finns ett tillämpligt undantag från det förbud mot sådan behandling som annars gäller enligt 13 §. Däremot har bestämmelserna i 9 och 10 §§ betydelse för om en direktåtkomst är tillåten och vilken omfattning den i så fall kan ha. Bestämmelser om direktåtkomst kan också påverka en myndighets informationsskyldighet enligt lagen. Skyldigheten att självmant lämna information till den registrerade om behandling av personuppgifter kan helt bortfalla om det finns en bestämmelse om direktåtkomst, men skyldigheten att lämna s.k. 26 §-utdrag kvarstår även om en sådan bestämmelse finns.

Vi har ovan berört frågan att det torde vara av avgörande betydelse att lämpliga säkerhetsåtgärder vidtas för att det integritetsskydd som är avsett att finnas vid en direktåtkomst också blir förverkligat. Något krav på att i olika hänseenden införa regler som fyller ut bestämmelserna i 31 § PuL om skyldighet att vidta lämpliga säkerhetsåtgärder finns det emellertid inte. Däremot följer av 32 § att Datainspektionen i enskilda fall kan besluta om säkerhetsåtgärder och av 50 b §§ att regeringen kan besluta föreskrifter om vilka krav som ställs på den personuppgiftsansvarige. Regeringen har vidaredelegerat föreskriftsrätten till Datainspektionen, men inspektionen har hittills inte meddelat några föreskrifter om säkerhetsåtgärder.

I prop. 2007/08:160 om ett utökat elektroniskt informationsutbyte anförde regeringen att en god informationssäkerhet vid myndigheterna är ett ständigt pågående utvecklingsarbete (s. 64 f.).

Riksrevisionen, som ansåg att aktuella myndigheter inte uppfyllde kraven på god informationssäkerhet, hade i sitt remissvar avseende det betänkande som propositionen byggde på (SOU 2007:45) föreslagit att någon form av certifiering borde krävas innan en myndighet tilläts delta i informationsutbytet. Enligt regeringen fick problem med bristande informationssäkerhet tas om hand i annan ordning och utgjorde inte hinder för att genomföra ett utökat elektroniskt informationsutbyte. Regeringen erinrade också om vikten av att berörda myndigheter lever upp till gällande krav på att vidta de tekniska och organisatoriska åtgärder som krävs till skydd för de personuppgifter som behandlas.

Även om en direktåtkomst alltså kan ha betydelse vid tillämpningen av personuppgiftslagen kan något krav på författningsstöd för att en direktåtkomst ska kunna etableras knappast härledas ur den lagen. Inte heller kan, som vi ser det, något sådant krav härledas ut dataskyddsdirektivet.

Finns krav på reglering i andra författningar?

Det kan konstateras att det inte heller av bestämmelserna i 4 och 5 kap. OSL följer något krav på att reglera en direktåtkomst. Upptagningar som en mottagande myndigheten får tillgång till genom direktåtkomst är emellertid att anse som utlämnade till myndigheten och utgör därmed allmänna handlingar. En myndighet har därför en skyldighet att upprätta en beskrivning som bl.a. ger information om hur de allmänna handlingar som är tillgängliga genom direktåtkomsten kan sökas fram. (4 kap. 2 § första stycket 2). Genom direktåtkomst torde också ett regelbundet inhämtande eller utlämnande av uppgifter ske. Beskrivningen bör därför också innehålla information om hur åtkomsten är ordnad samt vilka uppgifter den omfattar (4 kap. 2 § andra stycket 6).

Något krav på att registrera de allmänna handlingar som direktåtkomsten omfattar finns dock inte. Det ankommer enbart på den utlämnande myndigheten att registrera handlingarna (5 kap. 1 § andra stycket OSL).

Våra överväganden och förslag

Förslag och bedömning: Någon allmän regel om krav på författningsstöd för direktåtkomst bör inte införas. Däremot föreslås den nya lagen innehålla en bestämmelse som föreskriver att direktåtkomst till sekretessreglerade personuppgifter ska ha stöd i lag eller förordning. Från bestämmelsens tillämpningsområde undantas direktåtkomst som medges den registrerade eller dennes ombud och som tar sikte på uppgifter som hänför sig till den registrerade, som medges till uppgifter som är sekretessreglerade enligt 21 kap. 7 § OSL, som medges ett personuppgiftsbiträde eller som medges en myndighet endast för sådan teknisk bearbetning eller teknisk lagring som avses i 2 kap. 10 § första stycket TF för den utlämnande myndighetens räkning.

Det bör inte införas bestämmelser som innebär ett generellt krav på särskilt författningsstöd för direktåtkomst

Det kan konstateras att det inte finns något krav enligt gällande rätt på att direktåtkomst ska ha stöd i författning för att vara tillåten. Av vissa lagstiftningsärenden där registerförfattningar på olika områden har införts framgår emellertid att förslagen om bestämmelser om direktåtkomst bygger på ett antagande om att ett sådant stöd bör finnas. På somliga områden har det även införts bestämmelser som uttryckligen innebär att direktåtkomst bara är tillåten om den föreskrivs i lag eller förordning. Bortsett från sådana nyss nämnda områden där det sektorsvis införts krav på författningsstöd strider det alltså i dag inte mot någon bestämmelse att en myndighet på eget initiativ tillåter en annan myndighet eller någon annan aktör att få direktåtkomst till myndighetens informationssamlingar.

Det kan vidare konstateras att i de fall direktåtkomst har reglerats föreskrivs i de allra flesta fall att direktåtkomst ”får” medges. Ett undantag finns i den nya lagen (2014:484) om en databas för övervakning av och tillsyn över finansmarknaderna, som trätt i kraft den 1 augusti 2014. I den föreskrivs att direktåtkomst i vissa fall ”ska” medges. Att direktåtkomst ”får” medges innebär att den utlämnande myndigheten inte är skyldig att faktiskt anordna den

direktåtkomst som regleringen i och för sig medger. I förarbeten har anförts att innebörden av en sådan författningsreglering är att den myndighet som angetts få ha direktåtkomst inte har en ovillkorlig rätt att få ut uppgifterna, utan att den myndighet som innehar informationen har en rätt att medge sådan åtkomst (prop. 2011/12:45 s. 133). Den utlämnande myndigheten har ett principiellt ansvar att förvissa sig om att den myndighet som beviljas direktåtkomst vidtar de åtgärder som bedöms vara nödvändiga från säkerhetssynpunkt. Det påpekades vidare att detta förhållande tydliggörs i några författningar genom bestämmelser som anger att myndigheten i fråga inte får medge andra direktåtkomst till sina register innan den har försäkrat sig om behörighets- och säkerhetsfrågorna är lösta på ett sätt som är tillfredsställande från integritetssynpunkt. Ett annat exempel på liknande förarbetsuttalanden kan hämtas från prop. 2008/09:96 där regeringen framhöll att det är viktigt att den utlämnande myndigheten försäkrar sig om att mottagaren tillgodoser de krav som följer av personuppgiftslagen med avseende på lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifterna innan myndigheten rent faktiskt medger direktåtkomst till uppgifter i sin databas för olika användare (s. 63).

I de allra flesta fall där direktåtkomst har reglerats i en författning är det alltså den utlämnande myndigheten som ytterst förfogar över frågan om en direktåtkomst rent faktiskt ska komma till stånd. Detta får enligt vår mening uppfattas som en smidig och effektiv ordning, eftersom det då står den utlämnande myndigheten fritt att välja på vilket sätt uppgiftsutbytet ska ske utifrån vad som är möjligt och lämpligt.

Det ovan anförda ger enligt vår mening vid handen att det saknas skäl att införa generella bestämmelser som innebär att en direktåtkomst aldrig skulle vara tillåten utan särskilt författningsstöd. Vi föreslår därför inte någon sådan generell regel.

Direktåtkomst till sekretessreglerade uppgifter bör kräva stöd i lag eller förordning

Vi har i våra överväganden i frågan om det bör behållas en begreppsmässig åtskillnad mellan direktåtkomst och annat elektroniskt utlämnande framhållit att direktåtkomst är en betydligt mer vittomfattande form av elektroniskt utlämnande än andra sådana utläm-

nanden (se avsnitt 5.7). Att direktåtkomst är speciell illustreras av att varje sådan åtkomst i sig ger upphov till krav på att det övervägs om tillräcklig sekretess hos den mottagande myndigheten finns och om det finns en sekretessbrytande regel som möjliggör det utlämnande av uppgifter som direktåtkomsten innebär. Om det saknas sådana bestämmelser måste de införas i förväg. Av hänsyn till frågor om skydd för personuppgifter i allmänhet och informationssäkerhet samt fördelning av ansvar – både för verksamheten i stort och för personuppgifter – som väcks i samband med direktåtkomst är det också av stor vikt att även dessa frågor, liksom frågor om begränsning av överskottsinformation, är genomlysta och att de åtgärder som behövs har vidtagits innan direktåtkomsten etableras. Detta gäller i synnerhet när det är fråga om uppgifter som skyddas av regler om sekretess.

Även om vi alltså inte föreslår något generellt krav på författningsstöd för direktåtkomst talar enligt vår mening samma skäl som talar för att det också i fortsättningen bör göras en åtskillnad mellan begreppen direktåtkomst och annat elektroniskt utlämnande för att det bör införas ett uttryckligt krav på att direktåtkomst till sekretessreglerade personuppgifter ska ha stöd i lag eller förordning för att vara tillåten.

Det kan dock konstateras att det redan i dag följer av bestämmelserna i offentlighets- och sekretesslagen att en sekretessbrytande regel måste finnas för att ett utlämnande av sekretessreglerade uppgifter som sker genom direktåtkomst inte ska strida mot bestämmelser om sekretess. Det finns alltså redan ett krav på att det vid direktåtkomst införs en sekretessbrytande bestämmelse i lag eller förordning som möjliggör åtkomsten, om en sådan bestämmelse saknas. Det kan hävdas att det mest ingripande med en direktåtkomst är just nödvändigheten av att undanröja eventuella sekretesshinder så att gränsen mellan de inblandande myndigheterna öppnas upp. Det skulle i så fall tala för att det är tillräckligt att det redan finns ett krav på att undanröja sådana hinder genom en bestämmelse i författning.

Enligt vår uppfattning är det emellertid inte enbart behovet av en sekretessbrytande bestämmelse som gör att direktåtkomst särskiljer sig från andra former av elektroniska utlämnanden. Inte minst viktig är den omständigheten att den mottagande myndigheten bildligt talat släpps in innanför den andra myndighetens

dörrar. Denna omständighet, som innebär att myndigheterna i viss mån sammanför sina verksamheter, har betydelse inte bara för de sekretessfrågor som uppstår utan även för integritetsskydd i vidare mening samt för frågor om fördelning av verksamhetsansvar, exempelvis beträffande informationssäkerhet och rent förvaltningsrättsliga skyldigheter. Dessutom tillkommer alltså det förhållandet att i den mån en direktåtkomst i sig ger upphov till behov av författningsändringar det krävs att dessa har vidtagits på förhand, dvs. innan åtkomsten faktiskt etableras. Även för det fall det redan skulle finnas en tillämplig sekretessbrytande bestämmelse talar dessa omständigheter enligt vår uppfattning för att – i vart fall såvitt avser direktåtkomst till sekretessreglerade personuppgifter – avvägningarna inte uteslutande bör ske på myndighetsnivå. Det finns behov av överblick över rättsområdet och ett intresse av att verka för enhetlighet som talar för detta, inte minst när det gäller avvägningar mellan effektivitet och integritet men också i fråga om på vilken nivå kraven på t.ex. informationssäkerhet vid denna typ av uppgiftsutbyten bör ligga. Visserligen ställer bestämmelser i personuppgiftslagen och offentlighets- och sekretesslagen vissa krav på både den myndighet som medger direktåtkomst och den myndighet som använder sig av den, exempelvis att direktåtkomsten ska uppfylla grundläggande krav för och vara en tillåten behandling av personuppgifter samt att åtkomsten ska beskrivas i olika dokument som enskilda kan ta del av. Detta utgör emellertid endast krav som ska uppfyllas på myndighetsnivå och svarar därför inte mot de behov av överblick och enhetlighet som vi anser finns på området.

Vi anser därför att det finns ett behov av att i den nya lagen införa en bestämmelse som föreskriver att direktåtkomst till sekretessreglerade personuppgifter ska ha författningsstöd i lag eller förordning. Som vi kommer att utveckla närmare nedan torde enligt vår mening detta författningsstöd normalt sett kunna ges av regeringen, dvs. genom föreskrift i förordning. Med lag bör, i enlighet med den uppfattning som uttalats i samband med annan lagstiftning, kunna likställas en EU-förordning (se prop. 1999/2000:126 s. 272 och 283).

Enligt vår uppfattning är det alltså tillräckligt att begränsa den nu aktuella bestämmelsens tillämpningsområde till de fall då en direktåtkomst tar sikte på sekretessreglerade uppgifter. Visserligen

kan även direktåtkomst till uppgifter som inte skyddas av regler om sekretess, dvs. offentliga uppgifter, ge upphov till frågor om skydd för personuppgifter i en vidare mening. Även behov av genomlysning av frågor om fördelning av verksamhetsansvar uppstår vid en sådan åtkomst. Enligt vår uppfattning är emellertid en direktåtkomst till offentliga personuppgifter inte av samma känsliga art som en åtkomst som avser sekretessreglerade uppgifter. Dessutom torde det många gånger vara så att de fördelar från effektivitetssynpunkt som en direktåtkomst innebär uppenbart överväger de motstående intressen som kan finnas när det är fråga om offentliga uppgifter. Enligt vår uppfattning är det därför som huvudregel tillräckligt att de överväganden som behöver göras vid sådan åtkomst sker på myndighetsnivå, se avsnitt 10.1.4 angående vårt förslag om krav på den utlämnande myndigheten att göra en risk- och sårbarhetsanalys och träffa överenskommelse med mottagare om bl.a. säkerhetsåtgärder till skydd för personuppgifterna.

Kravet på författningsstöd vid direktåtkomst ska alltså inte gälla beträffande uppgifter som inte är sekretessreglerade utan offentliga. Vi återkommer nedan till frågan om det däremot behövs en bestämmelse som begränsar en myndighets möjlighet att medge direktåtkomst till offentliga uppgifter.

Av den inventering vi har gjort av de nuvarande registerförfattningarna kan man dra slutsatsen att en ny bestämmelse som föreskriver ett uttryckligt krav på författningsstöd i princip inte kommer att medföra några omedelbara konsekvenser för normgivaren, eftersom det redan i dag torde vara så att direktåtkomster som omfattar sekretessreglerade uppgifter har författningsstöd. Det förefaller alltså vara så att lagstiftaren redan har som utgångspunkt att det bör finnas ett sådant stöd. Genom den nya bestämmelsen kommer det emellertid att stå klart att det är en sådan ordning som gäller.

Undantag från kravet på författningsstöd

Sekretess till skydd för en enskild gäller som huvudregel inte i förhållande till den enskilde själv (jfr 12 kap. 1 § OSL). Från bestämmelsens tillämpningsområde bör därför undantas direktåtkomst som medges den registrerade och som tar sikte på uppgifter som hänför sig till honom eller henne själv (jfr definitionen

av personuppgifter i 3 § PuL). Inte heller bör det krävas stöd i författning för att medge den registrerades ombud direktåtkomst. Det förutsätter emellertid att det finns ett behov av de uppgifter som kan lämnas ut genom direktåtkomsten för den angelägenhet som ombudets behörighet avser. Det ankommer således på den utlämnande myndigheten att kontrollera att det förhåller sig på detta sätt innan en registrerads ombud medges direktåtkomst.

Även direktåtkomst till uppgifter som regleras av sekretess enligt 21 kap. 7 § OSL, dvs. den s.k. PuL-sekretessen, bör undantas. Som den bestämmelsen är formulerad kan den uppfattas innebära att alla personuppgifter som finns hos en myndighet är sekretessreglerade, eftersom alla personuppgifter kan komma att bli behandlade enligt personuppgiftslagen hos en presumtiv mottagare. Om den nya bestämmelsen med krav på författningsstöd för direktåtkomst till sekretessreglerade uppgifter skulle omfatta även 21 kap. 7 § OSL skulle det alltså innebära att all direktåtkomst måste ha författningsstöd. Ett undantag med avseende på den bestämmelsen är därför nödvändigt.

I sammanhanget kan även nämnas att det hos myndigheter i vars verksamhet det normalt inte förekommer sekretessreglerade uppgifter kan tillfälligtvis finnas uppgifter som är sekretessreglerade enligt exempelvis 21 kap. 1 § eller 21 kap. 3 § OSL. I dessa fall rör det sig om fall där sekretess gäller för uppgifterna oavsett i vilken myndighetsverksamhet de förekommer, dvs. sekretessen följer med uppgifterna. När sekretessen är konstruerad på detta sätt rör det sig normalt om ett särskilt kvalificerat skyddsintresse. Om sådana uppgifter förekommer hos en myndighet måste en direktåtkomst, som avses ta sikte på offentliga uppgifter, givetvis ordnas så att den inte omfattar också de skyddade uppgifterna. I annat fall krävs alltså författningsstöd för direktåtkomsten.

Från bestämmelsen med krav på författningsstöd för direktåtkomst till sekretessreglerade uppgifter bör det också införas ett undantag som tar sikte på den situationen då ett personuppgiftsbiträde ska få direktåtkomst till en myndighets informationssamlingar. Ett personuppgiftsbiträde får enligt 30 § första stycket PuL endast behandla personuppgifter i enlighet med instruktioner från den personuppgiftsansvariga myndigheten. Biträdet får alltså inte behandla de personuppgifter som biträdet får åtkomst till för något eget ändamål. I en sådan situation saknas alltså skäl att åstad-

komma det särskilda skydd för sekretessreglerade personuppgifter som kravet på författningsstöd avser att åstadkomma. Ett undantag för direktåtkomst som medges personuppgiftsbiträden bör därför införas.

Det förekommer också att en myndighet har direktåtkomst till upptagningar för att ha dessa i sitt förvar enbart som led i en teknisk bearbetning eller en teknisk lagring för en annan myndighets räkning. Enligt 2 kap. 10 § första stycket TF anses sådana handlingar inte vara allmänna hos den mottagande myndigheten. Något krav på författningsstöd för en sådan direktåtkomst bör enligt vår mening inte uppställas. I de fall en enskild aktör medges direktåtkomst till sekretessreglerade uppgifter i syfte att utföra motsvarande uppgifter kan det förutsättas att det sker med stöd i ett personuppgiftsbiträdesavtal. Den situationen omfattas således av det undantag från kravet på författningsstöd som tar sikte på direktåtkomst som medges personuppgiftsbiträden.

11.1.3 En ny regel som generellt bryter sekretess vid direktåtkomst för myndigheter

Problem med de sekretessbrytande bestämmelser som finns i dag

Eftersom de uppgifter som en direktåtkomst omfattar är att anse som utlämnande i och med att åtkomsten medges, måste åtkomsten – om den omfattar sekretessreglerade uppgifter hos den utlämnande myndigheten – möjliggöras genom en sekretessbrytande regel. Genomgången av befintliga registerförfattningar visar att regler om direktåtkomst i de allra flesta fall inte formuleras så att de i sig bryter sekretess, dvs. att direktåtkomst ”ska” medges. En sådan regel skulle däremot vara att se som en sådan uppgiftsskyldighet som avses i 10 kap. 28 § OSL och som i sig är sekretessbrytande. Ett enstaka exempel på detta är, som har framgått ovan, bestämmelserna om direktåtkomst i den nya lagen (2014:484) om en databas för övervakning av och tillsyn över finansmarknaderna. Men som huvudregel har alltså en direktåtkomst ansetts förutsätta att den kan förenas med en bestämmelse om uppgiftsskyldighet som omfattar de sekretessreglerade uppgifter som åtkomsten tar sikte på.

Det har i vissa förarbeten antytts att direktåtkomst kan förenas med ett utlämnande enligt den s.k. generalklausulen i 10 kap. 27 § OSL (se t.ex. prop. 2010/11:45 s. 143 och Lagrådets uttalande i prop. 2000/01:33 s. 347). Den s.k. generalklausulen förutsätter emellertid att en intresseavvägning görs. En sådan avvägning kan visserligen göras på förhand om man bedömer att ett utlämnande är möjligt även utan en avvägning i enskilda fall. Ett rutinmässigt utlämnande för en viss tid är då i och för sig möjligt. Så är emellertid inte alltid fallet. Även om ett rutinmässigt utlämnande med stöd av generalklausulen bedöms möjligt för en viss tid, är det ändå så att den utlämnande myndigheten i princip är oförhindrad att göra en ny bedömning i sekretessfrågan och besluta att ett utlämnande i ett enskilt fall inte ska ske. Den utlämnande myndigheten behåller alltså den rättsliga befogenheten att avgöra om uppgifter ska lämnas ut eller inte. Mot denna bakgrund förefaller ett utlämnande med stöd av generalklausulen inte kunna möjliggöra ett utlämnande genom direktåtkomst. När direktåtkomsten väl har etablerats har ju den utlämnande myndigheten inte längre kvar en rättslig befogenhet att pröva vilka uppgifter som i enskilda fall ska lämnas ut inom ramen för åtkomsten, eftersom uppgifterna redan anses utlämnande. Däremot torde den utlämnande myndigheten alltjämt ha en befogenhet att ta tillbaka medgivandet till direktåtkomst.

Av inventeringen av registerförfattningarna framgår att det inte har reglerats konsekvent hur och i vilken utsträckning det finns en uppgiftsskyldighet eller någon annan sekretessbrytande regel som knyter an till en bestämmelse om direktåtkomst. De uppgiftsskyldigheter som avses tillämpas är många gånger generellt utformade och tar inte särskilt sikte på direktåtkomsten. En annan iakttagelse är att det kan vara svårt att hitta de sekretessbrytande regler som avses möjliggöra direktåtkomsten. Så är exempelvis delvis fallet med de direktåtkomster som i 114 kap. SFB har medgetts till socialförsäkringsdatabasen. Det förekommer att en sekretessbrytande regel finns i en annan författning än den där direktåtkomsten regleras utan att någon hänvisning görs. Är frågan om sekretessbrytande regler inte heller uttryckligen behandlad i förarbetena, blir det mycket svårt att skaffa sig en bild av hur direktåtkomsten är tänkt att kunna ske utan att bryta mot gällande sekretess. På socialförsäkringsområdet har t.ex. under senare tid en uppgiftsskyl-

dighet för Försäkringskassan i förhållande till arbetslöshetskassorna upphävts, medan bestämmelsen som medger arbetslöshetskassorna direktåtkomst finns kvar trots att åtkomsten alltså inte längre kan användas. Det kan konstateras att den hittills tillämpade ordningen med separata bestämmelser som medger direktåtkomst respektive är sekretessbrytande har medfört att rättsområdet blivit mycket svåröverskådligt, även för lagstiftaren, och att den reglering som förekommer delvis är inkonsekvent.

Tekniken för att införa sekretessbrytande bestämmelser

Av 8 kap. 1 § OSL följer att sekretessbrytande bestämmelser som gäller i förhållande till andra myndigheter kan införas i offentlighets- och sekretesslagen eller i lag eller förordning som den lagen hänvisar till.

Som exempel på sekretessbrytande bestämmelser som införts direkt i offentlighets- och sekretesslagen och som avser att möjliggöra direktåtkomst kan nämnas 25 kap. 11 § 3, vilken bryter hälso- och sjukvårdssekretessen enligt samma kapitel för uppgifter som utbyts inom systemet för sammanhållen journalföring. Ett annat exempel är den nya sekretessbrytande bestämmelsen i 30 kap. 8 a § OSL som avses möjliggöra direktåtkomst till den nya databasen för övervakning av och tillsyn över finansmarknaderna (prop. 2013/14:161). Dessa bestämmelser har inte utformats som uppgiftsskyldigheter, utan föreskriver direkt i offentlighets- och sekretesslagen att sekretess inte hindrar det utlämnande av uppgifter som avses ske genom direktåtkomsten. När det gäller det sistnämnda lagstiftningsärendet kan konstateras att de bestämmelser som medger direktåtkomst i den föreslagna lagen om behandling av uppgifter i den nya databasen i sig är utformade som uppgiftsskyldigheter, eftersom de föreskriver att direktåtkomst ”ska” medges. Eftersom bestämmelserna i sig är sekretessbrytande föreslog 2011 års utredning av finansmarknadsstatistiken inte någon ytterligare bestämmelse (SOU 2012:79 s. 106 f.). I prop. 2013/14:161 konstaterar regeringen att de föreslagna bestämmelserna om direktåtkomst är utformade som uppgiftsskyldigheter, vilka enligt 10 kap. 28 § OSL medför att sekretessen bryts (s. 56). Enligt regeringen bör emellertid föreskrifter om sekretessgenombrott och föreskrif-

ter om på vilket sätt uppgifter lämnas ut, exempelvis genom direktåtkomst, ges i olika bestämmelser. Till skillnad från utredningen föreslog regeringen därför att det utöver bestämmelserna om direktåtkomst infördes en särskild sekretessbrytande bestämmelse i offentlighets- och sekretesslagen. Man kan emellertid göra den reflektionen att med bestämmelser som medger direktåtkomst, där det uttrycks att sådan åtkomst ”ska” medges, förefaller det knappast vara nödvändigt att också införa en särskild sekretessbrytande bestämmelse för att åstadkomma en sådan effekt. Av den utformning bestämmelserna om direktåtkomst har fått följer ju att de är sådana uppgiftsskyldigheter som enligt 10 kap. 28 § OSL bryter sekretess.

Möjligheten enligt 8 kap. 1 § OSL att införa en sekretessbrytande bestämmelse genom en hänvisning i den lagen till en bestämmelse i annan lag eller förordning används oftast i fråga om sekretessbrytande bestämmelser som tar sikte på enskildas möjlighet att ta del av uppgifter, exempelvis 27 kap. 7 § och 28 kap. 6 §. Då det gäller sekretessbrytande bestämmelser som gäller i förhållande till andra myndigheter används vanligen i stället den möjlighet som ges genom den generellt sekretessbrytande bestämmelsen i 10 kap. 28 § OSL. Den föreskriver att sekretess inte hindrar att uppgifter lämnas till en annan myndighet om det finns en uppgiftsskyldighet i lag eller förordning. I så fall behövs det ingen hänvisning i offentlighets- och sekretesslagen till den aktuella lagen eller förordningen. Om denna möjlighet används, kan alltså både en bestämmelse som medger direktåtkomst och den sekretessbrytande bestämmelsen som behövs för att möjliggöra åtkomsten föras in i t.ex. en registerförfattning utan att någon ändring behöver göras i offentlighets- och sekretesslagen. Det torde vara förklaringen till att flertalet av de sekretessbrytande bestämmelser som avser att möjliggöra direktåtkomst för andra myndigheter har utformats som just uppgiftsskyldigheter.

Våra överväganden och förslag

Förslag: I 10 kap. OSL införs det en generellt sekretessbrytande bestämmelse som innebär att föreskrifter i lag eller förordning om direktåtkomst för myndigheter i sig får en sekretessbrytande effekt. Därigenom behöver det inte längre införas särskilda sekretessbrytande bestämmelser för att möjliggöra direktåtkomst enligt den ordning som i dag vanligtvis tillämpas. Den nya bestämmelsen bör knyta an till den definition av begreppet direktåtkomst som vi förordar. Bestämmelsen bör inte omfatta direktåtkomst som medges utländska myndigheter eller enskilda.

När man överväger att underlätta ett uppgiftsutbyte mellan myndigheter genom direktåtkomst får det från integritetsskyddssynpunkt alltså anses centralt att frågan om behovet av sekretessbrytande bestämmelser blir föremål för noggranna avvägningar så att en sådan bestämmelse inte blir onödigt vid. Det är också av stor betydelse att det klart framgår av en ny reglering vilket utbyte av uppgifter som utan hinder av sekretess får förekomma genom en direktåtkomst och hur åtkomsten får användas. Vi har alltså kunnat konstatera att den hittills tillämpade ordningen med separata bestämmelser som medger direktåtkomst respektive är sekretessbrytande har medfört att rättsområdet blivit mycket svåröverskådligt och att den reglering som förekommer delvis är inkonsekvent. I syfte att åstadkomma en klargörande reglering skulle enligt vår uppfattning mycket stå att vinna om man i offentlighets- och sekretesslagen genom en generellt gällande bestämmelse kunde föreskriva att en bestämmelse om direktåtkomst i sig är sekretessbrytande. I så fall skulle en bestämmelse som medger direktåtkomst inte behöva förenas med en särskild sekretessbrytande bestämmelse, exempelvis i form av en uppgiftsskyldighet. En sådan ordning förordades av Lagrådet redan år 2000 i samband med införandet av registerförfattningar på skatteområdet (prop. 2000/01:33 s. 347). Lagrådet anförde att det var önskvärt att en formell överensstämmelse åstadkoms mellan registerlagarna och sekretesslagen så att sekretessbrytande effekt av föreskrifter om direktåtkomst regleras i anslutning till dåvarande 14 kap. 1 och 3 §§ sekretesslagen (numera 10 kap. 28 respektive 27 §§ OSL).

Förklaringen till att flertalet av de sekretessbrytande bestämmelser som har införts i registerförfattningar för att möjliggöra direktåtkomst har utformats som uppgiftsskyldigheter torde, som vi redan konstaterat, vara att det då inte behöver föras in någon hänvisning i offentlighets- och sekretesslagen till den sekretessbrytande bestämmelsen. En uppgiftsskyldighet syftar emellertid i grunden inte till att bryta sekretess utan kan ha avfattats utan tanke på att avse just hemliga uppgifter. Det grundläggande syftet är snarare att göra klart att en myndighet är skyldig att lämna en viss uppgift till en annan myndighet utan att någon prövning får ske. Motsatsvis finns en ovillkorlig rätt för den andra myndigheten att få uppgifterna. Som exempel kan nämnas bestämmelsen i 13 kap. 1 § RF som föreskriver att konstitutionsutskottet har rätt att få de handlingar från regeringen som utskottet finner nödvändigt för sin granskning. Bestämmelsen utvidgades genom 2010 års grundlagsändringar till att avse också andra handlingar hos regeringen än sådana som hör till regeringsärenden. I förarbetena konstaterades att 6 kap. 5 § OSL och den sekretessbrytande bestämmelsen i 10 kap. 15 § samma lag, som föreskriver att sekretess inte hindrar att en uppgift lämnas till riksdagen eller regeringen (prop. 2009/10:80 s. 114 f.) i och för sig innebar en långtgående skyldighet för regeringen att på begäran av konstitutionsutskottet tillhandahålla utskottet uppgifter i andra handlingar än sådana som tillhör regeringsärenden. Regeringen framhöll att utskottet dock inte kunde grunda någon uttrycklig rätt att få tillgång till sådana handlingar p.g.a. bestämmelserna om kontrollmakten i dåvarande 12 kap. 1 § RF (numera 13 kap. 1 §), som då endast omfattade handlingar i regeringsärenden. En sådan uttrycklig rätt borde därför införas, vilket alltså skedde genom en utvidgning av tillämpningsområdet för regeringens uppgiftsskyldighet gentemot utskottet vid dess granskning.

Vid direktåtkomst är det normalt de inblandade myndigheterna som gemensamt kommer överens om hur åtkomsten i praktiken ska ordnas och ytterst den utlämnande myndigheten som beslutar att ”släppa in” den mottagande myndigheten i sina uppgiftssamlingar. I och med att direktåtkomsten faktiskt har etablerats, är de uppgifter som omfattas utlämnande till den myndigheten. Att uppgifterna lämnas ut är alltså en faktisk och rättslig konsekvens av att direktåtkomsten verkställs. Och detta är i sin tur alltså en följd av

den utlämnande myndighetens beslut även om etableringen av direktåtkomsten förutsätter viss samverkan med den mottagande myndigheten för att förbereda åtkomsten tekniskt och på andra sätt. Vid direktåtkomst är det således normalt sett inte fråga om en situation där det finns ett behov av att klargöra att den utlämnande myndigheten har en skyldighet att lämna ut uppgifter respektive att den mottagande myndigheten har en ovillkorlig rätt att få ut uppgifterna.

Är inblandade myndigheter väl överens om att direktåtkomsten faktiskt kan etableras, blir utlämnandet alltså ett resultat av denna överenskommelse. En uppgiftsskyldighet i en särskild sekretessbrytande bestämmelse kan visserligen vara en förutsättning men är inte i sig styrande för att en överenskommelse om direktåtkomst faktiskt ska komma till stånd. Situationen blir förstås annorlunda om det i bestämmelsen om direktåtkomst föreskrivs att sådan åtkomst ”ska” medges. En sådan bestämmelse fungerar ju som styrande både för att åtkomsten faktiskt ska komma till stånd och för att sekretessen ovillkorligen bryts. Som redan framhållits är denna typ av bestämmelse mycket ovanlig, i allmänhet reglerar man endast att direktåtkomst ”får medges”. Det ankommer alltså i de allra flesta fall på den utlämnande myndigheten att besluta om huruvida direktåtkomsten i praktiken ska medges. I en sådan situation finns det således inget behov av att den sekretessbrytande bestämmelsen ska ha formen av en uppgiftsskyldighet, utan det räcker med att den har en sekretessbrytande effekt.

Som vi redan framhållit torde förklaringen till att det är just formen uppgiftsskyldighet som i allmänhet ändå har valts som sekretessbrytande bestämmelse vid direktåtkomst vara att man då slipper ändringar i offentlighets- och sekretesslagen. Enligt vår mening är det emellertid principiellt sett otillfredsställande att den sekretessbrytande effekt som krävs vid direktåtkomst åstadkoms genom att man inför regler som föreskriver en uppgiftsskyldighet som kanske sakligt sett inte alls behövs och som dessutom kanske inte efterlevs i den mån direktåtkomst av något skäl inte kommer till stånd. En bestämmelse som, utan att hänvisa till uppgiftsskyldighet, direkt i offentlighets- och sekretesslagen föreskriver att sekretess inte hindrar att uppgift lämnas till en myndighet som har medgetts direktåtkomst till en annan myndighets uppgiftssamlingar skulle således på ett betydligt bättre sätt åstadkomma den sekre-

tessbrytande effekt som behövs vid sådan åtkomst. Vi föreslår därför att det införs en sådan bestämmelse.

I enlighet med bestämmelserna i 8 kap. 1 § OSL bör den nya bestämmelsen hänvisa till en direktåtkomst som medgetts i lag eller förordning. En sådan formulering stämmer också överens med den bestämmelse som vi föreslår ska införas i den nya lagen om myndigheters behandling av personuppgifter, vilken föreskriver att direktåtkomst till sekretessreglerade personuppgifter inte är tillåten utan ett uttryckligt stöd i lag eller förordning. Eftersom den nya bestämmelsen i offentlighets- och sekretesslagen syftar till att vara generellt sekretessbrytande bör den införas i 10 kap. Då den avser att bryta sekretess vid direktåtkomst för andra myndigheter oavsett i vilken verksamhet direktåtkomsten förekommer kan den lämpligen införas som ett nytt andra stycke i 10 kap. 28 §. Bestämmelsen bör knyta an till den definition av begreppet direktåtkomst som vi förordar, dvs. att det ska vara frågan om sådan teknisk tillgång till upptagningar hos en annan myndighet som avses i 2 kap. 3 § andra stycket TF.

Enligt sin nuvarande utformning tar 10 kap. 28 § OSL enbart sikte på att reglera när sekretess inte ska gälla i förhållande till svenska myndigheter. Detsamma bör gälla i fråga om den sekretessbrytande bestämmelsen vid direktåtkomst som nu föreslås. I fråga om direktåtkomst som medges utländska myndigheter får i stället bestämmelsen i 8 kap. 3 § OSL tillämpas. Enligt den bestämmelsen gäller inte sekretess i förhållande till en utländsk myndighet eller en mellanfolklig organisation om utlämnandet sker i enlighet med särskild föreskrift i lag eller förordning. Med lag likställs EU-förordningar (Lenberg m.fl., kommentaren till 8 kap. 3 §).

Genom att bestämmelsen görs generellt tillämplig i de fall en myndighet ska få medges direktåtkomst kommer den att vara sekretessbrytande också i förhållande till brottsbekämpande myndigheter. Den kommer också att bryta sekretess i fråga om uppgifter som inte är personuppgifter. Visserligen ingår det inte i vårt uppdrag att överväga vad som ska gälla i fråga om behandling av personuppgifter hos brottsbekämpande myndigheter och inte heller att överväga ny reglering av andra uppgifter än personuppgifter. Enligt våra direktiv är vi emellertid oförhindrade att ta upp andra frågor än de som nämns i direktiven, om vi anser att dessa behöver regleras för att uppdraget ska kunna fullgöras på ett tillfredsställ-

ande sätt. Den föreslagna sekretessbestämmelsen kan enligt vår mening knappast ges en tillfredsställande utformning om den inte görs generell på detta sätt.

Den föreslagna generellt sekretessbrytande bestämmelsen tar alltså sikte på de fall då direktåtkomst har medgetts en annan svensk myndighet. Den kommer alltså inte att omfatta också de fall då enskilda har tillåtits få en sådan åtkomst. Det kan konstateras att det är ovanligt att enskilda bereds möjlighet att genom direktåtkomst ta del av sekretessreglerade uppgifter. Det finns således inget egentligt behov av att införa en generellt sekretessbrytande regel för sådana fall. Flertalet av de generellt sekretessbrytande bestämmelserna som införts i 10 kap. tar också sikte på utlämnande av uppgifter till myndigheter. Enligt vår uppfattning bör det därför inte föreslås någon motsvarande bestämmelse som gäller till förmån för enskilda. I den mån en sekretessbrytande bestämmelse behövs för att möjliggöra en direktåtkomst för enskilda måste det således också i fortsättningen göras en ändring i offentlighets- och sekretesslagen, antingen i form av att en särskild sekretessbrytande bestämmelse införs eller att en hänvisning görs till en sådan bestämmelse i annan lag eller förordning.

11.1.4 Hur bestämmelser om direktåtkomst med sekretessbrytande effekt bör utformas

En förenkling av regelverket kring direktåtkomst

Om det införs en bestämmelse i offentlighets- och sekretesslagen som föreskriver att direktåtkomst som tillåtits i lag eller förordning i sig har en sekretessbrytande effekt finns det alltså inte längre ett behov av att en bestämmelse om direktåtkomst förenas med en särskild sekretessbrytande bestämmelse. Det innebär att det i fortsättningen inte behöver införas några särskilda sekretessbrytande bestämmelser i samband med att det enligt lag eller förordning tillåts nya direktåtkomster för myndigheter. Vidare kan, då gällande registerförfattningar ses över, sådana särskilda sekretessbrytande bestämmelser som har införts för att möjliggöra en viss direktåtkomst upphävas, eftersom de inte längre behövs förutsatt att själva direktåtkomsten har författningsstöd. Frågan blir då vilka krav som bör ställas på regler genom vilka direktåtkomst medges.

Innan vi går in på den saken finns det skäl att något beröra en särskild avgränsningsfråga.

I en del registerförfattningar har det införts uppgiftsskyldigheter som syftar till att komplettera den sekretessbrytande bestämmelse som avses möjliggöra direktåtkomsten. Det anses finnas behov av ett sådant komplement för det fall att det p.g.a. tekniska problem inte går att använda sig av direktåtkomst (prop. 2010:11/78 s. 21). Därigenom avses det bli möjligt att i stället lämna ut uppgifterna via telefon eller e-post. Som exempel på en sådan bestämmelse om kompletterande uppgiftsskyldighet kan nämnas 4 § första stycket andra meningen förordningen (2001:588) om behandling av uppgifter i Skatteverkets beskattningsverksamhet.

Vid en direktåtkomst är samtliga de uppgifter som omfattas av åtkomsten att anse som utlämnade till den mottagande myndigheten i den stund åtkomsten etableras. Om det därefter uppstår tekniska problem som innebär att det tillfälligtvis inte är möjligt att via den tekniska anslutningen göra en faktisk överföring av uppgifter i ett konkret fall och uppgifterna i stället överförs manuellt via exempelvis telefon eller e-post, förefaller det enligt vår mening långsökt att se detta som ett nytt utlämnande som i så fall rättsligt sett sker utanför direktåtkomsten. Ett annat synsätt skulle kunna vara att den utlämnande myndigheten i detta fall hjälper den mottagande myndigheten med att genomföra den faktiska överföringen, eftersom uppgifterna rättsligt redan har lämnats ut till den myndigheten. Med ett sådant synsätt skulle det alltså fortfarande vara fråga om en faktisk överföring av uppgifter inom ramen för en redan beviljad direktåtkomst, låt vara att den vid ett visst tillfälle behöver ske med en manuell hjälpinsats från den utlämnande myndigheten.

Om man ändå väljer att betrakta ett manuellt utlämnande som behöver ske då direktåtkomsten inte fungerar som ett i formell mening nytt utlämnande, torde det ändå vara så att detta kan ske med stöd av den s.k. generalklausulen i 10 kap. 27 § OSL. Direktåtkomst är ju den mest ingripande formen för ett uppgiftsutbyte. Om en bestämmelse som tillåter en sådan åtkomst har införts, vilken kompletterats med en sekretessbrytande bestämmelse som möjliggör åtkomsten eller är sekretessbrytande i sig, bör det inte vara något problem att kunna konstatera att den intresseavvägning som ska göras vid en tillämpning av den s.k. generalklausulen får till

resultat att ett utlämnande är möjligt för att lösa en tillfällig problemsituation som har uppstått inom ramen för direktåtkomsten. Med stöd av 10 kap. 27 § OSL bör uppgifter alltså tillfälligtvis kunna överföras också manuellt i ett enskilt fall. Här bör dock uppmärksammas att den bestämmelsen inte gäller i fråga om viss sekretess enligt de lagrum som räknas upp i paragrafen. I dessa undantagsfall kan alltså eventuellt en kompletterande uppgiftsskyldighet behövas om direktåtkomst medges på dessa sekretessområden och det av oss nyss förespråkade betraktelsesättet inte anläggs.

Enligt vår uppfattning finns alltså som huvudregel inte något behov av kompletterande uppgiftsskyldigheter som syftar till att vara någon slags ”back up” i den händelse direktåtkomsten av tekniska skäl inte kan användas vid ett visst tillfälle. Vi anser därför att den generellt sekretessbrytande bestämmelsen som vi föreslår ska införas i 10 kap. OSL är tillräcklig för att bryta sekretess även då direktåtkomsten inte fungerar och att – i den mån ett momentant manuellt utlämnande inte betraktas som en del av den redan etablerade direktåtkomsten – i vart fall 10 kap. 27 § OSL kan användas då en direktåtkomst tillfälligtvis drabbas av tekniska problem. Det innebär att sådana uppgiftsskyldigheter som enbart har till syfte att komplettera en sekretessbrytande bestämmelse som ska möjliggöra direktåtkomst med vårt förslag framöver i princip kan avvaras.

Eftersom en bestämmelse om direktåtkomst i sig blir sekretessbrytande ställs krav på att den har en tillräcklig konkretion

Vårt förslag till en ny generellt sekretessbrytande bestämmelse innebär alltså att bestämmelser om direktåtkomst i sig kommer att styra i vilken omfattning uppgifter kan lämnas ut genom direktåtkomst utan hinder av sekretess. Det medför i sin tur ett krav på att sådana bestämmelser formuleras så att åtkomstens omfattning och därmed dess sekretessbrytande effekt beskrivs på ett tydligt sätt. Formuleringen måste syfta till att beskriva omfattningen så att den täcker samtliga slags uppgifter som den utlämnande myndigheten gör tekniskt åtkomliga för den mottagande myndigheten, eftersom alla dessa uppgifter lämnas ut i den stund åtkomsten faktiskt etableras.

I gällande författningar används olika former av formuleringar för att beskriva vilken direktåtkomst som får medges en myndighet eller enskild aktör. Ibland görs en uppräkning av vilka uppgifter åtkomsten får omfatta. Som exempel kan nämnas 2 kap. 7–9 §§ lagen (2001:181) om behandling av uppgifter i Skatteverkets beskattningsverksamhet. Där anges, med hänvisning till andra paragrafer, vilka slags uppgifter som genom direktåtkomst får vara tillgängliga för Skatteverkets brottsutredande verksamhet, Kronofogdemyndigheten, Tullverket och socialnämnder. Genom en sådan formulering blir det tydligt vilken omfattning åtkomsten har. En sådan bestämmelse skulle därför även i sig kunna fungera som en sekretessbrytande bestämmelse. Ett annat exempel på en bestämmelse som på ett tydligt sätt beskriver en direktåtkomsts omfattning och som i sig skulle kunna ha en sekretessbrytande effekt är 8 § lagen (2006:444) om passagerarregister. I den paragrafen föreskrivs att Säkerhetspolisen får för sådan verksamhet som anges i en annan paragraf ha direktåtkomst till personuppgifterna i passagerarregistret. Den korresponderande uppgiftsskyldigheten i 6 § har också en i princip likalydande formulering.

När det gäller direktåtkomst till socialförsäkringsdatabasen har emellertid en annan typ av formulering använts. I 114 kap. 19–23 §§ SFB föreskrivs att angivna aktörer får ha direktåtkomst till databasen i den utsträckning åtkomsten behövs för de ändamål som beskrivs i bestämmelserna. Dessa bestämmelser syftar alltså till att föreskriva för vilka behov åtkomsten får användas och inte till att beskriva vilken omfattning åtkomsten får ha. I förordningen (2003:766) om behandling av personuppgifter inom socialförsäkringens administration finns i 3–4 §§ bestämmelser som kompletterar vissa av de direktåtkomster som medges i 114 kap. 19–23 §§ SFB. Där beskrivs antingen vilka uppgifter direktåtkomsten får omfatta eller hänvisas till uppgiftsskyldigheter som följer av någon annan författning. I de fall en beskrivning lämnas av vilka uppgifter direktåtkomsten får omfatta finns det emellertid inte någon kompletterande sekretessbrytande bestämmelse i förordningen. De uppgiftsskyldigheter som avser att bryta sekretessen i dessa fall finns i stället i andra författningar, men någon hänvisning lämnas inte till dem i förordningen. När det gäller socialförsäkringsdatabasen har alltså direktåtkomstens omfattning och kompletterande sekretessbrytande bestämmelser reglerats på tre olika ställen och i vissa fall

utan att någon hänvisning mellan de olika regelverken har gjorts. Det kan också konstateras att det i ”portalparagraferna” om direktåtkomst i 114 kap. SFB inte regleras vilken omfattning direktåtkomsten får ha, vilket alltså är den huvudsakliga frågan som behöver regleras genom denna typ av bestämmelser, utan i stället hur direktåtkomsten får användas. Regler om hur direktåtkomsten får användas fungerar främst som styrande för vilka uppgifter som i enskilda fall får sökas fram och överföras genom åtkomsten. Bestämmelserna om direktåtkomst i 114 kap. SFB skulle alltså inte kunna fungera som föreskrifter som på ett tillräckligt tydligt sätt bryter sekretess vid sådan åtkomst. Det är i stället snarare bestämmelserna i nämnda förordning som beskriver vilken omfattning i vart fall vissa av direktåtkomsterna har.

Omfattningen av några av de direktåtkomster som medges till socialförsäkringsdatabasen regleras emellertid inte heller i den ovan nämnda förordningen. Det rör direktåtkomsterna för Statens tjänstepensionsverk och KPA Pension AB. För Statens tjänstepensionsverk torde den korresponderande uppgiftsskyldigheten finnas i förordningen (1980:995) om skyldighet för Försäkringskassan och Pensionsmyndigheten att lämna uppgifter till andra myndigheter. Där sägs dock endast i 2 § att uppgifter ska lämnas på begäran om de behövs för ärenden enligt vissa uppräknade författningar. Inte heller av denna bestämmelse framgår alltså vilken omfattning direktåtkomsten för Statens tjänstepensionsverk får ha, utan endast för vilka behov en överföring får ske i enskilda fall. Frågan är också om denna typ av uppgiftsskyldighet över huvud taget bryter sekretess på ett sådant sätt att en direktåtkomst är möjlig. För KPA Pension AB:s del finns sekretessbrytande bestämmelser som eventuellt kan möjliggöra bolagets direktåtkomst i 28 kap. 6 § OSL och 110 kap. 39 § SFB. Det går emellertid inte heller att mot bakgrund av dessa bestämmelser få en bild av vilken omfattning direktåtkomsten får ha, utan endast för vilket behov uppgifter får lämnas ut i ett enskilt fall.

Vi kan bara konstatera att oavsett om en generellt sekretessbrytande bestämmelse införs eller inte, det inte kan anses tillfredsställande att det är så komplicerat att skaffa sig en bild av vilken omfattning direktåtkomsterna till socialförsäkringsdatabasen har. När det gäller direktåtkomsterna för Statens tjänstepensionsverk och KPA Pension AB kan det ifrågasättas om gällande bestäm-

melser över huvud taget reglerar vilken omfattning direktåtkomsten får ha. En förklaring till att bestämmelserna har utformats på detta otillfredsställande sätt kan vara att man har ansett det tillräckligt att använda de uppgiftsskyldigheter som har funnits sedan tidigare, dvs. innan ett uppgiftsutbyte fick ske i formen av direktåtkomst utan som då skedde genom att uppgifter lämnades ut på begäran i enskilda fall efter en manuell bedömning. Om man inte har gjort klart för sig vilken omfattning en direktåtkomst avses ha, är det emellertid knappast möjligt att ta ställning till om det redan finns en sekretessbrytande bestämmelse som möjliggör direktåtkomsten eller om en ny sådan bestämmelse behöver införas.

Såväl i fråga om gällande regelverk som beträffande tillämpningen av den föreslagna generellt sekretessbrytande bestämmelsen är det således av stor vikt att regelverket ger ett tydligt svar på vilken omfattning en direktåtkomst får ha. Det är alltså inte tillräckligt att reglerna endast ger svar på i vilken utsträckning direktåtkomsten får användas i konkreta fall inom ramen för åtkomsten. I den mån bestämmelser om direktåtkomst har formulerats på det sätt som använts i fråga om socialförsäkringsdatabasen finns det därför enligt vår mening under alla förhållanden ett behov av att se över regelverket för att åstadkomma en tillräcklig tydlighet i fråga om åtkomstens omfattning.

Den av oss föreslagna generellt sekretessbrytande bestämmelsen har således den positiva effekten att den tvingar fram tydlighet och innebär en förenkling av regelverket. Bestämmelsen innebär alltså att en regel som medger direktåtkomst samtidigt kommer att ha en sekretessbrytande effekt. Därmed ställs det krav på lagstiftaren att ge bestämmelsen om direktåtkomst en tillräcklig konkretion. Eftersom en och samma bestämmelse både medger direktåtkomst och bryter sekretess skapas vidare ett betydligt mer lättöverskådligt regelverk där inkonsekvenser enklare kan undvikas. Att åstadkomma bättre överskådlighet och tydlighet får anses särskilt betydelsefullt både för att upprätthålla ett tillfredsställande skydd för personuppgifter vid direktåtkomst och för att skapa ett regelverk som är avsevärt lättare att tillämpa för myndigheterna.

Bestämmelser om hur direktåtkomsten får användas är också viktiga för att uppnå ett tillfredsställande integritetsskydd

Bestämmelser om direktåtkomst innehåller också ofta regler om hur direktåtkomsten får användas, t.ex. för vilka behov uppgifter får överföras eller i vilken typ av ärenden som uppgifter får samlas in genom åtkomsten. Sådana regler är också viktiga för att ett tillfredsställande integritetsskydd ska åstadkommas. De styr emellertid inte vilken omfattning direktåtkomsten får ha och riktar sig alltså inte mot den utlämnande myndigheten. I stället ger de den mottagande myndigheten besked om hur dess tjänstemän får använda sig av den direktåtkomst som myndigheten som sådan har medgetts. Föreskrifter av det slaget kan alltså tjäna som underlag för på vilken behörighetsnivå som åtkomsten får användas i enskilda fall och för vilken typ av ärenden. Därmed kan de också vara styrande för vilka begränsningar i form av teknisk åtkomst som den mottagande myndigheten kan behöva åstadkomma inom ramen för sitt eget system. Det förekommer att man i regler om direktåtkomst även föreskriver att den mottagande myndigheten inte får medges någon direktåtkomst förrän den utlämnande myndigheten har försäkrat sig om att den myndigheten har åstadkommit de åtkomstbegränsningar som behövs. Så är exempelvis fallet med socialnämndernas direktåtkomst till beskattningsdatabasen och socialförsäkringsdatabasen (2 kap. 8 a § lagen [2001:181] om behandling av uppgifter i Skatteverkets beskattningsverksamhet och 114 kap. 22 och 23 §§ SFB). I förarbetena till nämnda bestämmelser betonade regeringen att det inte är rimligt att ställa upp krav på att de myndigheter som föreslås få rätt att medge socialnämnderna direktåtkomst själva ska vidta kontroller av landets alla socialnämnder (prop. 2007/08:160 s. 150). Någon skyldighet att genomföra faktiska kontroller avsågs inte heller med förslaget. Enligt regeringen torde det vara tillräckligt att man inhämtar en försäkran från den mottagande socialnämnden om att de krav som uppställs är uppfyllda.

Det är således viktigt att bestämmelser om direktåtkomst också innehåller regler om hur åtkomsten får användas i enskilda fall, men denna typ av regler bör som vi ser det på ett tydligt sätt skiljas från de regler som syftar till att beskriva vilken omfattning direktåtkomsten får ha. Medan den förstnämnda regeltypen har den

mottagande myndigheten som adressat, riktar sig den sistnämnda till utlämnande myndighet som får rätt att eller, vilket är betydligt mer ovanligt, blir skyldig att medge direktåtkomst av en viss given omfattning.

Kan en skyldighet att lämna ut uppgifter ”på begäran” möjliggöra direktåtkomst?

Det är vanligt att bestämmelser om direktåtkomst kompletteras av en skyldighet att lämna ut uppgifter som innebär att den utlämnande myndigheten ”på begäran” ska lämna ut uppgifter om de behövs i ett visst ärende. Som exempel har ovan redan nämnts uppgiftsskyldigheten till förmån för Statens tjänstepensionsverk i 2 § förordningen (1980:995) om skyldighet för Försäkringskassan och Pensionsmyndigheten att lämna uppgifter till andra myndigheter. Det förefaller enligt vår mening mycket tveksamt om denna typ av uppgiftsskyldighet bryter sekretess på ett sådant sätt att de kan möjliggöra ett uppgiftsutbyte genom direktåtkomst. Äldre uppgiftsskyldigheter som har formulerats på detta sätt har inte heller haft till syfte att möjliggöra direktåtkomst, utan har införts för att klargöra att den mottagande myndigheten eller annan aktör har en rätt att få ut uppgifter då det begärs i ett enskilt fall.

Att denna typ av uppgiftsskyldighet utgör ett problem i samband med direktåtkomst uppmärksammades i förarbetena till bestämmelserna om att Kronofogdemyndigheten får medges direktåtkomst till uppgifter i Skatteverkets beskattningsdatabas för skuldsaneringsändamål (prop. 2010/11:78). Regeringen konstaterade att den gällande uppgiftsskyldigheten i 36 § skuldsaneringslagen (2006:548), som föreskriver att socialnämnder och andra myndigheter till Kronofogdemyndigheten eller domstol som handlägger ärenden om skuldsanering på begäran ska överlämna sådana uppgifter om gäldenärens personliga och ekonomiska förhållanden som behövs för prövning av ärendet, inte var lämpad att ligga till grund för en bestämmelse om direktåtkomst (a. prop. s. 20). Den sekretessbrytande bestämmelsen borde i stället formuleras som en rätt för den mottagande myndigheten att ta del av vissa specificerade uppgifter hos den utlämnande myndigheten utan att det ställs upp krav på att varje enskild uppgift ska ha betydelse i ett enskilt ärende.

Det förekommer emellertid fortfarande att det införs uppgiftsskyldigheter för att möjliggöra direktåtkomst där det föreskrivs att uppgifter ska lämnas ut på begäran för ett visst behov hos den mottagande myndigheten. Som exempel kan nämnas de nya bestämmelserna i mönstringslagen (1983:929), som trädde i kraft den 3 juli 2014, som möjliggör direktåtkomst till sjömansregistret (23 a §) och som tillåter Transportstyrelsen att medge sådan åtkomst (23 b §).

Normgivningsnivån när det gäller föreskrifter om direktåtkomst

När det gäller direktåtkomst innebär vårt förslag till en ny lag om personuppgiftsbehandling på myndighetsområdet alltså inte att den lagen i sig kommer att reglera i vilka fall direktåtkomst kan eller får medges. Det den nya lagen ska innehålla är en bestämmelse som föreskriver att stöd för direktåtkomst till sekretessreglerade uppgifter som huvudregel ska finnas i lag eller förordning. Om sådan direktåtkomst ska medges, måste det alltså ske i form av särregler.

I avsnitt 7.3 har vi utförligt redovisat hur vi ser på frågan om normgivningsnivå för särregler i förhållande till den generella lagen, bl.a. vad gäller direktåtkomst. Vi har där kommit till den slutsatsen att den omständigheten att direktåtkomst medges normalt inte i sig innebär att det sker något ingrepp i enskilds personliga förhållanden i den mening som avses i 8 kap. 2 § första stycket 2 RF. Föreskrifter om att direktåtkomst får medges bör därför i de allra flesta fall kunna ges i form av förordning. Om direktåtkomsten emellertid förutsätter att enskildas sekretesskydd i realiteten försvagas på så sätt att känsliga personuppgifter kan lämnas ut i betydligt större omfattning än vad som annars hade varit möjligt kan det vara att anse som ett sådant ingrepp i enskildas personliga förhållanden som förutsätter att författningsstödet för direktåtkomsten ges i lag.

Vi har också framhållit att av betydelse för om en direktåtkomst kan anses utgöra ett ingrepp i enskilds personliga förhållanden är vilket förhållande de myndigheter har till varandra mellan vilket uppgiftsutbytet sker. Om myndigheternas verksamheter har nära anknytning till varandra och förutsätter att ett visst uppgiftsutbyte sker för att respektive myndighet ska kunna utföra sina uppgifter talar det för att en direktåtkomst mellan dessa myndigheter inte i

sig utgör ett ingrepp i enskilds personliga förhållanden. Om däremot exempelvis brottsbekämpande myndigheter medges direktåtkomst till sekretessreglerade personuppgifter hos myndigheter som inte ägnar sig åt brottsbekämpning torde det ofta vara frågan om ett ingrepp i enskilds personliga förhållanden som kräver stöd i lag, såvida inte uppgiftsutbytet är av ringa omfattning.

De omständigheter kring hur personuppgifter har samlats in till en myndighet, bl.a. när det gäller ändamålet för insamlingen, och karaktären på uppgifterna kan således leda till en bedömning att en direktåtkomst får anses utgöra ett sådant ingrepp i enskilds personliga förhållanden som avses i 8 kap. 2 § första stycket 2 RF och som i så fall kräver stöd i lag. I de allra flesta fall utgör direktåtkomst emellertid en metod för att effektivisera ett uppgiftsutbyte som redan äger rum. De registrerade kan då i objektiv mening inte anses ha någon berättigad förväntan på att det särskilda skydd som lagformen innebär behöver aktualiseras. Direktåtkomst kan då tillåtas med stöd av förordning.

Vi har också bedömt att det förefaller vara i rena undantagsfall som behandling av personuppgifter hos myndigheter som inte ägnar sig åt brottsbekämpning kan anses innehålla moment som typiskt sett kan anses som en sådan kartläggning eller övervakning som innebär ett betydande intrång i den personliga integriteten i den mening som avses i grundlagsstadgandet i 2 kap. 6 § andra stycket RF. Stadgandet – som trädde i kraft den 1 januari 2011 – har hittills såvitt avser direktåtkomst tillämpats i ett fall. Det gällde den reglering som innebär att EU:s medlemsstater ska ha sådan åtkomst till varandras nationella DNA-, fingeravtrycks- och fordonsregister (se prop. 2010/11:129 s. 49 f.).

Sammanfattningsvis gör vi alltså bedömningen att man som huvudregel kan utgå från att det krav på författningsstöd som ska gälla enligt den generella lagen för direktåtkomst till sekretessreglerade uppgifter kan åstadkommas på förordningsnivå, dvs. genom föreskrifter som meddelas av regeringen.

11.1.5 Finns det anledning att begränsa en myndighets möjlighet att medge direktåtkomst till offentliga uppgifter?

Bakgrund

Vi har ovan föreslagit att det införs en bestämmelse som föreskriver att direktåtkomst till sekretessreglerade personuppgifter ska ha stöd i lag eller förordning. I det sammanhanget har vi bedömt att det som huvudregel är tillräckligt att de överväganden som behöver göras innan en direktåtkomst medges till uppgifter som inte är sekretessreglerade utan offentliga sker på myndighetsnivå. Det finns dock anledning att fråga sig om det, förutom de grundläggande krav och bestämmelser om vad som är en tillåten behandling som finns i personuppgiftslagen och som ska gälla också enligt den nya lagen, bör införas någon särskild bestämmelse som begränsar en myndighets möjlighet att medge sådan direktåtkomst.

Det kan konstateras att det förekommer att även direktåtkomst till offentliga uppgifter är föremål för författningsreglering. Ett sådant exempel är bestämmelsen om direktåtkomst i 8 § lagen (2001:558) om vägtrafikregister. Enligt den bestämmelsen får direktåtkomst endast medges för sådana ändamål som anges i 5 § 1–3 och 7 samma lag. Det innebär att de mottagare som får medges direktåtkomst för vissa särskilt angivna ändamål är stat och kommun, försäkringsgivare eller annan allmän eller enskild verksamhet där vissa angivna uppgifter utgör underlag för prövningar och beslut samt viss utländsk myndighet. Utan att specificera vilka mottagare som avses får direktåtkomst även medges till information om fordonsägare för trafiksäkerhets- eller miljöändamål och för att i den allmänna omsättningen av fordon förebygga brott. Information om behörighet att framföra körkort får även lämnas genom direktåtkomst för att utreda trafikbrott i samband med automatisk trafiksäkerhetskontroll.

I förarbetena till bestämmelserna om direktåtkomst i lagen om vägtrafikregister anförde regeringen att några problem från integritetssynpunkt, såvitt känt, inte förelåg med den dåvarande tillgången till uppgifter via direktåtkomst (prop. 2000/01:95 s. 80). Det fanns därför inget skäl att införa förbud mot sådan åtkomst. Integritetsaspekterna gjorde sig emellertid starkt gällande när det gällde möjligheterna till direktåtkomst och det var viktigt att det alltjämt

förekom begränsningar i fråga om sådan åtkomst. Regeringen hänvisade därvid till att Datainspektionen i sitt remissvar anfört att det av integritetsskäl behövs gränser för i vilken utsträckning terminalåtkomst ska få förekomma till uppgifterna i vägtrafikregistret och att det borde anges i lagen att direktåtkomst endast får ske i omfattning som regeringen bestämmer. Regeringen instämde i att frågan om möjlighet till direktåtkomst inte enbart skulle överlåtas på den personuppgiftsansvarige utan borde regleras i författning. Det borde därför tas in en bestämmelse i lagen som begränsar möjligheterna att medge direktåtkomst till de för personuppgifter särskilt angivna ändamålen i enlighet med föreskrifter meddelade av regeringen. Direktåtkomst borde dock inte tillåtas om syftet med åtkomsten är att komplettera eller kontrollera kund- eller medlemsregister eller om syftet är att göra en s.k. urvalsdragning.

I förordningen (2001:650) om vägtrafikregister finns kompletterande bestämmelser om direktåtkomst. I 4 kap. 3 § definieras vad som avses med direktåtkomst i 8 § lagen om vägtrafikregister. Sådan åtkomst är för handen när användare av registret via elektronisk överföring på det sätt som Transportstyrelsen föreskriver har möjlighet att direkt eller via informationsförmedlare söka i vägtrafikregistret och där få svar på frågor.

Vidare föreskrivs i 4 kap. 4 § första stycket förordningen att direktåtkomst till uppgifter i vägtrafikregistret endast får medges om den utgör en tillåten behandling av personuppgifter enligt personuppgiftslagen. Direktåtkomst får inte medges innan Transportstyrelsen försäkrat sig om att behörighets- och säkerhetsfrågorna är lösta på ett sätt som är tillfredsställande ur integritetssynpunkt. Enligt andra stycket får ett medgivande återtas om förutsättningarna för det inte längre finns eller om det finns någon annan särskild anledning att återta det.

I 4 kap. 5 § första stycket finns en uttömmande uppräkning av vilka sökbegrepp som andra användare än en statlig eller kommunal myndighet får beviljas rätt att använda för sökning i registret. Enligt andra stycket medges Transportstyrelsen rätt att bestämma ytterligare begränsningar av användningen av sökbegrepp och de övriga villkor som bedöms nödvändiga ur integritetssynpunkt.

Förordningen innehåller också bestämmelser om direktåtkomst enligt Prümrådsbeslutet, vilka inte behandlas vidare här.

Ett annat exempel på att man gett uttryckligt stöd för direktåtkomst till offentliga uppgifter genom en författningsreglering är aktiebolagsregistret. Enligt 2 kap. 1 § första stycket aktiebolagsförordningen (2005:559) ska registret ge offentlighet åt den information som ingår i registret. Det är alltså huvudändamålet med registret. I andra stycket finns en uppräkning av för vilka ändamål registret ska tillhandahålla personuppgifter, exempelvis för affärsverksamhet, kreditgivning eller annan verksamhet där företagsanknuten information utgör underlag för prövningar eller beslut eller för förvärv, avyttring eller förvaltning av företag som registreras i aktiebolagsregistret. Vidare föreskrivs i 4 § att Bolagsverket får medge direktåtkomst till registret för de ändamål som anges i 1 §.

Bestämmelserna om direktåtkomst till aktiebolagsregistret infördes år 2002 genom ändringar i den dåvarande förordningen (1975:1387). Frågan om direktåtkomst har inte behandlats i några förarbeten till aktiebolagslagen, där bestämmelser om att aktiebolagsregistret ska föras finns i 27 kap. (prop. 2004/05:85 s. 491). Det kan konstateras att som bestämmelsen om direktåtkomst har formulerats i aktiebolagsförordningen torde sådan åtkomst som omfattar personuppgifter vara begränsad till de ändamål som anges i andra stycket, medan direktåtkomst till andra uppgifter kan användas utan avgränsning.

Även förslaget till en ny domstolsdatalag innehåller bestämmelser om direktåtkomst till personuppgifter hos domstolarna. Eftersom förslaget inte innehåller vare sig något förslag till eller resonemang kring behovet av sekretessbrytande bestämmelser får åtkomsten antas avse uppgifter som inte är sekretessreglerade. Enligt förslaget får direktåtkomst medges en allmän domstol, en allmän förvaltningsdomstol eller en hyres- och arrendenämnd samt en part och en parts ombud, biträde eller försvarare såvitt avser personuppgifter i ett eget mål eller ärende (20 §). Vidare föreskrivs i förslaget till 21 § att regeringen eller den myndighet som regeringen bestämmer meddelar ytterligare föreskrifter om begränsning av direktåtkomsten enligt 20 § samt om behörighet och säkerhet vid sådan åtkomst.

I den promemoria där förslaget läggs fram konstateras att det i de databaser och register som förs av domstolarna ofta finns stora mängder personuppgifter, varav många kan vara av känslig karaktär (Ds 2013:10 s. 131). Ju fler personer som har omedelbar tillgång till

sådana uppgiftssamlingar, desto mer påtaglig är risken för intrång. Det påpekas att direktåtkomst också kan minska möjligheterna att kontrollera den vidare användningen av uppgifterna. Dessa förhållanden utgör skäl för en restriktiv hållning i fråga om direktåtkomst till uppgifter som domstolarna behandlar. När det gäller direktåtkomst till känsliga personuppgifter anförs i promemorian att det vore tveksamt att ge regeringen rätt att utvidga möjligheten till direktåtkomst till alla typer av uppgifter med hänsyn till de svåra avvägningar mellan integritetsskydd och effektivitetsintressen som bör ske. Det ifrågasätts också om en sådan möjlighet för regeringen att meddela föreskrifter om direktåtkomst skulle vara förenlig med 2 kap. 6 § RF. Enligt promemorian bör det därför regleras i den nya lagen i vilka fall direktåtkomst får medges.

Det kan konstateras att de föreslagna lagbestämmelserna emellertid inte innehåller några närmare regler om i vilka fall och i vilken omfattning direktåtkomst får medges. I bestämmelserna pekas endast ut för vilka mottagare direktåtkomst får medges. Vad gäller part och en parts ombud m.fl. sägs dock att möjligheten till direktåtkomst är begränsad till det egna målet eller ärendet. I övrigt föreskrivs inte till vilka uppgifter och hos vilken domstol de olika mottagarna får medges direktåtkomst. Avsikten är att regeringen eller den myndighet som regeringen bestämmer ska besluta om de närmare villkoren, exempelvis i fråga om vilka domstolar som ska få ha direktåtkomst hos vem och vilka uppgifter åtkomsten får avse (a.a. s. 134). I bestämmelserna uttrycks inte heller att det endast är de nämnda mottagarna som får medges direktåtkomst, även om det framgår av promemorian att detta är avsikten med bestämmelserna med undantag för åtkomst via ”allmänhetens terminal” (a.a. s. 134 f.).

Våra överväganden

Bedömning: Det saknas behov av en särskild bestämmelse som begränsar en myndighets möjlighet att medge direktåtkomst till offentliga uppgifter som förekommer i dess verksamhet. Den avvägning mellan effektivitetsintressen och integritetsskydd som behöver göras innan en sådan åtkomst medges kan ske med stöd av generella bestämmelser om grundläggande krav, tillåten behandling och krav på säkerhetsåtgärder.

De särskilda komplikationer som gör sig gällande vid direktåtkomst som omfattar sekretessreglerade uppgifter och som innebär att åtkomsten måste möjliggöras genom en sekretessbrytande regel uppstår alltså inte vid direktåtkomst till offentliga uppgifter. I ett sådant sammanhang finns det därmed inget behov av att överväga frågor om integritetsskydd i den bemärkelsen att en åtkomst avses omfatta uppgifter som är skyddade av sekretess. Bestämmelser i författning om direktåtkomst till offentliga uppgifter motiveras emellertid vanligen med att de behövs för att skydda de registrerades integritet i vidare mening. Ibland utvecklas det inte närmare vilket skyddsbehov som avses, såsom i fråga om vägtrafikregistret, medan det ibland ges en mer utförlig motivering. Som exempel kan nämnas förslaget till en ny domstolsdatalag, där man både åberopat att det är fråga om stora mängder personuppgifter, varav många kan vara av känslig karaktär samt att direktåtkomsten i sig medför risker. De risker som framhålls är att ju fler personer som har omedelbar tillgång till sådana uppgiftssamlingar, desto mer påtaglig är risken för intrång samt att direktåtkomst kan minska möjligheterna att kontrollera den vidare användningen av uppgifterna.

När det gäller förordningsbestämmelserna om direktåtkomst till aktiebolagsregistret framgår inte av några förarbeten varför de har införts. Eftersom direktåtkomsten har avgränsats på så sätt att det räknas upp för vilka behov personuppgifter får tillhandahållas, kan man anta att integritetsskyddsskäl ligger till grund för denna avgränsning.

Det är otvivelaktigt så att direktåtkomst i sig innebär en effektiv möjlighet att överföra uppgifter på så sätt att många personer kan ta del av alla de uppgifter som omfattas av åtkomsten utan att det vid varje enskild överföring av uppgifter krävs en arbetsinsats från den utlämnande myndighetens sida. Enligt vår uppfattning kan detta i sig emellertid knappast sägas innebära att det normalt sett uppstår ett behov av att skydda integriteten på grund av att risken för intrång ökar eller att möjligheterna att kontrollera den vidare användningen av uppgifterna försämras. Det finns alltså inget omedelbart samband mellan en direktåtkomst avseende offentliga uppgifter och ett ökat behov av att skydda enskildas integritet.

För att det ska finnas ett sådant samband torde för det första krävas att det handlar om uppgifter som är av sådan karaktär att det

alls finns anledning att tala om intrång när det gäller möjligheterna att ta del av dem. Om syftet med ett register är att ge offentlighet till de uppgifter som finns där kan man inte gärna hävda att det skulle innebära ett intrång att så effektivt som möjligt ordna åtkomsten till uppgifterna. För att det ska uppstå en risk för intrång måste således omständigheter kring hur uppgifterna har samlats in eller karaktären på uppgifterna medföra att de registrerade får anses ha en berättigad förväntan på att åtkomsten till uppgifter som rör dem i något avseende ska vara begränsad, exempelvis genom att direktåtkomst inte tillåts. Om det finns en risk för intrång, torde det också finnas ett behov av att kontrollera den vidare användningen av uppgifterna. Däremot förefaller det vara svårt att finna något exempel på en situation då det skulle finnas ett behov av att av integritetsskyddsskäl kontrollera den vidare användningen om någon intrångsrisk saknas.

Aktiebolagsregistret har inrättats för att ge offentlighet åt de uppgifter som finns där. Trots det har man i bestämmelser begränsat möjligheterna att ta del av personuppgifter i registret till vissa ändamål. I de uppräknade ändamålen förefaller man ha försökt fånga in för vilka behov det kan finnas skäl att begära ut uppgifter från registret. Man kan emellertid fråga sig på vilket sätt det skulle påverka integriteten för någon som är registrerad i aktiebolagsregistret att direktåtkomst till uppgifter som rör denne medges trots att den som använder sig av direktåtkomsten inte har något särskilt behov av att ta del av uppgifterna.

Det förefaller enligt vår uppfattning som om man många gånger närmast slentrianmässigt utgår från att direktåtkomst i sig medför risker för den enskildes integritet, dvs. även om sådan åtkomst enbart tar sikte på offentliga uppgifter. Att så är fallet är givet när det gäller sekretessreglerade uppgifter men resonemangen behöver nyanseras betydligt när det gäller offentliga uppgifter, i vart fall beträffande myndigheternas verksamhet.

Ett område där direktåtkomst däremot kan tänkas medföra en klar risk för intrång i enskildas integritet trots att det handlar om offentliga uppgifter är sådan åtkomst till personuppgifter som behandlas inom ramen för domstolarnas verksamhet. I den verksamheten gäller ett högre krav på öppenhet och möjlighet till insyn än i annan offentlig verksamhet genom bestämmelsen i 2 kap. 11 § andra stycket RF att förhandling vid domstol ska vara offentlig.

Regeln kan ses som en komplettering till informationsfriheten i 2 kap. 1 § första stycket 1 RF och rätten till allmänna handlingar enligt 2 kap. TF. Rättegångsoffentligheten ger garanti för att även övriga processuella principer följs (se Holmberg m.fl., kommentaren till 2 kap. 11 § RF).

I domstolarnas verksamhet gäller därför sekretess i mer begränsad utsträckning än vad som är fallet i myndigheters verksamhet. Det kan därför förekomma uppgifter i den verksamheten som är känsliga utan att de skyddas av någon bestämmelse om sekretess. Vidare har personuppgifter samlats hos domstolarna av skäl som kan uppfattas som känsliga för den enskilde, exempelvis att man är anklagad för ett brott eller att man är ett brottsoffer eller att man har hamnat i en tvist med en annan enskild eller någon myndighet. När det gäller domstolarnas avgöranden är möjligheterna att hemlighålla uppgifter genom sekretess ytterst begränsade, samtidigt som domstolarna kan behöva använda sig av känsliga personuppgifter för att på ett tillräckligt utförligt sätt motivera sina avgöranden. Trots att det finns ett synnerligen högt intresse av att domstolarnas avgöranden är offentliga, kan det alltså konstateras att en obegränsad direktåtkomst till avgörandena eller domstolarnas diarier torde innebära en beaktansvärd risk för intrång i enskildas integritet. Därmed finns det också ett behov av att kunna kontrollera att inte stora mängder av domstolarnas samlade offentliga information sprids för vilket ändamål som helst. I det sammanhanget kan konstateras att det enligt 21 § PuL som huvudregel är förbjudet för andra än myndigheter att behandla personuppgifter om lagöverträdelser som innefattar brott, domar i brottmål, straffprocessuella tvångsmedel eller administrativa frihetsberövanden.

Frånsett domstolarnas verksamhet kan det emellertid konstateras att det torde vara sällan som direktåtkomst till offentliga uppgifter kan sägas medföra en risk för intrång i enskildas integritet som är av det slaget att det kan vara motiverat att genom bestämmelser i författning begränsa möjligheterna att medge sådan åtkomst. Enligt vår uppfattning är det i flertalet fall tillräckligt att utlämnande myndighet gör de avvägningar som behövs med hänsyn till den enskildes integritet då myndigheten avser att medge direktåtkomst till offentliga uppgifter. En myndighet är ju väl medveten om vilka uppgifter som den ska utföra inom ramen för sin verksamhet, för vilka ändamål som personuppgifter samlas in eller

på annat sätt tillförs verksamheten och i vilken utsträckning de personer som förekommer i myndighetens verksamhet upplever denna som känslig för egen del. Enligt vår uppfattning har en utlämnande myndighet därför i allmänhet goda möjligheter att göra den nyanserade bedömning som behövs för att beakta både effektivitetsintressen och integritetsskydd. Det finns dock anledning att erinra om att det inte bara är för att upprätthålla ett tillräckligt integritetsskydd som det är av stor vikt att myndigheterna gör en noggrann och allsidig bedömning rörande tillhandahållanden av uppgifter genom direktåtkomst. Om en rimlig balans mellan effektivitetshänsyn och integritetsskydd inte upprätthålls kan det i sin tur leda till krav på mer sekretess och därmed försämrade möjligheter till insyn i myndigheternas verksamhet. Om offentliga uppgifter oreflekterat och rutinmässigt tillhandahålls på det sätt som kanske är snabbast, billigast och mest effektivt, kan det komma att mötas av berättigade krav på att uppgifterna i fråga i stället som huvudregel inte ska tillhandahållas alls utan hållas hemliga. Det ankommer alltså på utlämnande myndigheter att göra en noggrann avvägning så att en sådan utveckling motverkas.

Vi har redan ovan påpekat att även andra myndigheters direktåtkomst till offentliga uppgifter kan medföra att det uppstår ett behov av att genomlysa frågor som rör fördelning av verksamhetsansvar i stort och beträffande personuppgiftsansvar mellan de inblandade myndigheterna. I samband med direktåtkomst kan det också finnas anledning att ta ställning till att frågor om informationssäkerhet är tillräckligt beaktade. Det är mot den bakgrunden som vi i avsnitt 10.1.4 föreslagit att det införs ett krav i den nya lagen på att överenskommelser i sådana frågor ska träffas i samband med att direktåtkomst medges. Det kravet föreslås gälla vid direktåtkomst avseende såväl sekretessreglerade som offentliga personuppgifter. Dessa frågor är dock inte av sådan karaktär när det gäller uppgifter som inte är sekretessreglerade att det, vid sidan av de krav som redan följer av bl.a. förvaltningslagen och personuppgiftslagen, finns anledning att genom en särskild bestämmelse begränsa möjligheterna för en myndighet att medge en annan myndighet eller en annan aktör direktåtkomst till sådana uppgifter.

Någon bestämmelse som generellt begränsar myndigheters möjlighet att medge direktåtkomst till offentliga uppgifter som förekommer i dess verksamhet föreslås alltså inte.

Det står förstås lagstiftaren fritt att ändå införa sådana bestämmelser om det i något visst fall anses finnas ett behov av begränsningar i möjligheterna att medge direktåtkomst till offentliga uppgifter. Sådana föreskrifter torde undantagslöst kunna ges i förordningsform när det gäller statliga myndigheter. I fråga om kommuner kan en sådan bestämmelse däremot innebära ett åliggande. I lagen behövs därför ett bemyndigande som medger regeringen eller den myndighet som regeringen bestämmer att meddela sådana föreskrifter.

11.2 Behövs särskilda regler för annat elektroniskt utlämnande än direktåtkomst?

11.2.1 Nuvarande bestämmelser om elektroniskt utlämnande m.m.

Bestämmelser som innebär stöd för utlämnanden i elektronisk form m.m.

Förordningen om tiden för tillhandahållande av domar och beslut, m.m.

I förordningen (2003:234) om tiden för tillhandahållande av domar och beslut, m.m., den s.k. serviceförordningen, finns bestämmelser för domstolar och statliga förvaltningsmyndigheter som bl.a. avser hur handlingar tillhandahålls. Enligt 10 § får en handling skickas med telefax eller elektronisk post eller på annat sätt tillhandahållas i elektronisk form om det är lämpligt.

Den aktuella bestämmelsen infördes i samband med att ändringar gjordes i 2 kap. TF med hänsyn till informationsteknikens utveckling. I förarbetena till dessa ändringar anförde regeringen att det var högst otillfredsställande att vissa myndigheter fattat principbeslut om att över huvud taget inte lämna ut allmänna handlingar i elektronisk form (prop. 2001/02:70 s. 34 f.). I många fall torde det enligt regeringen i själva verket stå klart för en myndighet att ett utlämnande i elektronisk form inte medför risk för otillbörliga integritetsintrång. Det torde vidare ofta vara både effektivt och ändamålsenligt för såväl myndigheten som den enskilde om handlingen lämnas ut i sådan form. Regeringen aviserade mot den bak-

grunden sin avsikt att föra in en bestämmelse i serviceförordningen som erinrar om att allmänna handlingar får lämnas ut i elektronisk form om det är lämpligt.

PSI-direktivet och lagen om vidareutnyttjande av handlingar från den offentliga förvaltningen

Det s.k. PSI-direktivet (Europaparlamentets och rådets direktiv 2003/98/EG av den 17 november 2003 om vidareutnyttjande av information från den offentliga sektorn) har ett övergripande syfte att myndigheter ska främja vidareutnyttjande av offentlig information.

PSI-direktivet har genomförts i svensk rätt genom lagen (2010:566) om vidareutnyttjande av handlingar från den offentliga förvaltningen (PSI-lagen), som trädde i kraft den 1 juli 2010. Lagen gäller för handlingar hos både statliga och kommunala myndigheter. Den innehåller bestämmelser som avser att förhindra att myndigheter beslutar om sådana villkor för hur handlingar får användas som begränsar konkurrensen (1 § andra stycket).

I 1 § tredje stycket lämnas en upplysning om att bestämmelser om tillhandahållande av handlingar finns i andra författningar. Bestämmelsen syftar till att tydliggöra att lagen inte kan åberopas som grund för att handlingar ska lämnas ut (prop. 2009/10:175 s. 141). Å andra sidan är lagen tillämplig i det konkreta fall då en handling eller delar av en handling lämnas ut, oavsett på vilken rättslig grund detta sker.

Enligt 4 § första stycket gäller lagen inte för handlingar eller uppgifter i handlingar som inte får tillhandahållas eller för begränsningar i vidareutnyttjandet av dessa som en myndighet är skyldig att besluta om eller som följer av någon författning.

I förarbetena till 4 § konstaterade regeringen att den omständigheten att handlingar som omfattas av sekretess kan lämnas ut med förbehåll eller att registerförfattningar innehåller regler om att handlingar får lämnas ut i elektronisk form endast under vissa förutsättningar kan innebära att möjligheterna till vidareutnyttjande begränsas (a. prop. s. 142 f.). För att inte påverka skyddet för den personliga integriteten borde lagen emellertid inte påverka tillämpningen av bestämmelser som föreskriver att myndigheten måste begränsa vidareutnyttjandet.

Lagen gäller vidare inte för handlingar som en myndighet tillhandahåller en annan myndighet, utom när det framgår att handlingarna ska användas i affärsverksamhet (4 § andra stycket).

Enligt 8 § ska villkor för vidareutnyttjande vara relevanta och icke diskriminerande för jämförbara kategorier av vidareutnyttjande. Villkoren får inte i onödan begränsa möjligheterna till vidareutnyttjande.

I förarbetena till 8 § påpekas att begränsningar i tillhandahållandet av handlingar som följer av tryckfrihetsförordningen och offentlighets- och sekretesslagen samt personuppgiftslagen m.fl. författningar faller, som framgår av 4 § första stycket, utanför direktivets och lagens tillämpningsområde och utgör därför inte villkor i den mening som avses i lagen (a. prop. s. 166).

Europaparlamentet och rådet har den 26 juni 2013 beslutat om ändringar av PSI-direktivet. Ändringarna ska ha genomförts i medlemsstaterna senast den 18 juli 2015. Genom ändringsdirektivet har artikel 5, som inte ansetts krävs någon särskild reglering i svensk lagstiftning (Ds 2009:44 s. 50–51, prop. 2009/10:175 s. 159), formulerats om. Där föreskrivs nu att offentliga myndigheter ska göra sina handlingar tillgängliga i alla befintliga format och språkversioner samt, om möjligt och lämpligt, i ett öppet och maskinläsbart format tillsammans med tillhörande metadata. Både format och metadata bör så långt det är möjligt vara förenliga med formella öppna standarder. I sin tidigare lydelse föreskrevs i artikeln att myndigheter skulle se till att deras handlingar finns tillgängliga på elektronisk väg, om detta är möjligt och lämpligt. Den inskjutna satsen ”om detta är möjligt och lämpligt” har alltså flyttats och avser numera enbart valet av format.

PSI-utredningen konstaterade i sitt betänkande Ett steg vidare – nya regler och åtgärder för att främja vidareutnyttjande av handlingar (SOU 2014:10) att ändringarna i artikel 5 skulle kunna tolkas så att det förts in en mer undantagslös skyldighet att tillhandahålla handlingar elektroniskt jämfört med det ursprungliga direktivet (a. bet. s. 80). PSI-utredningen bedömer, med hänsyn till att tillämpningsbestämmelserna i artiklarna 1.3 och 1.4 fortfarande gäller, att så emellertid inte är fallet och att ändringarna i artikel 5 inte kräver någon lagändring. Utredningen vill dock påminna om det diskrimineringsförbud som redan gäller enligt 8 § PSI-lagen, vilket innebär att en myndighet inte kan bevilja elektroniskt utlämnande till en

vidareutnyttjare, men neka en annan, så länge det gäller jämförbara kategorier av vidareutnyttjande och ett utlämnande inte strider mot sekretess eller någon annan skyldighet för myndigheten (a. bet. s. 84).

Exempel på hur frågan om utlämnanden i elektronisk form regleras i några registerförfattningar

Frågan om elektroniska utlämnanden har hanterats på skilda sätt i olika registerförfattningar. Medan lagstiftaren på skatteområdet och i fråga om patientdata har gjort bedömningen att sekretessbestämmelserna och bestämmelser om vad som utgör en tillåten behandling av personuppgifter är tillräckliga för att skydda personuppgifter vid ett elektroniskt utlämnande som sker på begäran av en annan myndighet, har lagstiftaren i fråga om personuppgifter i socialförsäkringsdatabasen ansett att det behövs särskilda regler som begränsar ett sådant utlämnande. Skälet synes ha varit att det ansågs finnas en risk för att efterkommande behandlingar kan komma att strida mot finalitetsprincipen, dvs. bestämmelsen i 9 § första stycket d PuL, om ingen begränsning mot spridning från den utlämnande myndigheten infördes (prop. 2002/03:135 s. 99).

Även i fråga om utlämnanden från Centrala studiestödsnämnden har det införts begränsningar i möjligheterna att lämna ut personuppgifter i elektronisk form såväl till andra myndighet som till enskilda. Förutom de särskilda fall där ett elektroniskt utlämnande är möjligt, är ett sådant utlämnande också möjligt i enskilda fall i fråga om enstaka uppgifter (13 § studiestödsdatalagen [2009:287]). I fråga om denna begränsning anförde regeringen att det var främst vid ett systematiskt eller återkommande elektroniskt utlämnande av en större mängd personuppgifter som begränsningar är nödvändiga av integritetsskyddsskäl (prop. 2008/09:96 s. 65 f.).

I lagstiftningsärendet om behandling av personuppgifter i beskattningsverksamheten anlades alltså ett annat synsätt. Där konstaterades att myndigheter vanligen inte har rättsligt stöd för att behandla personuppgifter annat än i enlighet med de för myndigheten gällande författningarna. Någon risk för att mottagande myndigheter ska behandla personuppgifter som hämtas in på medium för automatiserad behandling på ett sätt som inte är avsett torde inte finnas (prop. 2000/01:33 s. 112 f.). Däremot ansåg regeringen att utlämnanden i elektronisk form till enskilda endast borde vara tillåtet

när det efter en särskild prövning anses lämpligt. Det var emellertid inte möjligt att i lag reglera i vilka fall en sådan möjlighet skulle finnas, utan det överlämnades till regeringen att göra dessa bedömningar. I 9 § förordningen (2001:588) om behandling av uppgifter i Skatteverkets beskattningsverksamhet anges att utlämnande till enskilda av uppgifter enligt 11–15 §§ får göras i elektronisk form, om det inte finns hinder mot det i någon författning. I de angivna paragraferna finns bestämmelser som medger utlämnande till kreditupplysningsföretag, trossamfund, den registrerade själv m.fl. trots den absoluta sekretess som gäller på skatteområdet.

När det gällde patientdatalagen framhölls i förarbetena att den stränga hälso- och sjukvårdssekretessen och motsvarande bestämmelser för den privata hälso- och sjukvården utgjorde ett starkt integritetsskydd. Ytterligare begränsningar för utlämnandet behövde därför inte införas (prop. 2007/08:126 s. 77). I stället ankom det på den utlämnande myndigheten att göra en lämplighetsprövning. Vid den prövningen borde hänsyn tas till vilka risker ur säkerhets- och integritetssynpunkt som finns och dessa vägas mot eventuella vinster ur effektivitetssynpunkt. Vad denna lämplighetsprövning närmare skulle ta sikte på berördes emellertid inte.

I de båda sistnämnda lagstiftningsärendena har man alltså inte sett något behov av att införa särskilda begränsningar mot utlämnanden till andra myndigheter på medium för automatiserad behandling för att motverka en antagen risk att mottagande myndighet skulle komma att behandla personuppgifter vid sidan av de ändamål som avsetts. Uttalandena i lagstiftningsärendet om patientdatalagen tar även sikte på elektroniska utlämnanden som sker på begäran från enskilda.

När det gäller passagerarregistret har lagstiftaren däremot infört ett uttryckligt förbud mot att lämna ut uppgifter elektroniskt. Förbudet träffar både Tullverket, som har rätt att på begäran få ut uppgifter från registret utan hinder av sekretess, och myndigheter till vilka uppgifter kan lämnas ut efter en intresseavvägning enligt 10 kap. 27 § OSL. I detta fall har lagstiftaren uppenbarligen inte ansett att sekretessregler och andra bestämmelser som styr myndigheters behandling av personuppgifter utgör ett tillräckligt skydd vid elektroniska utlämnanden som sker på begäran. Vilka närmare överväganden som gjorts i frågan framgår dock inte av förarbetena. Det kan emellertid konstateras att även i fråga om direktåtkomst

har man varit mycket återhållsam. Fram till 1 januari 2015 var det, trots att både polismyndigheter och Tullverket hade rätt att få ut uppgifter ur registret, endast polismyndigheter som fick medges direktåtkomst. Skälet synes vara att det endast var de som hade ansvaret för personalkontroll vid flygplatserna (jfr prop. 2005/06:129 s. 79). Om Tullverket eller någon annan myndighet skulle få ett sådant ansvar i framtiden, har regeringen getts möjlighet att meddela föreskrifter om att också den myndigheten ska få direktåtkomst.

Ett annat register som har ett mycket integritetskänsligt innehåll är belastningsregistret. Regeringen har i lagen (1998:620) om belastningsregister getts ett bemyndigande att meddela föreskrifter om direktåtkomst (6 § andra stycket). Direktåtkomst får medges de myndigheter som avses i 6 § första stycket, vilka är de myndigheter som har rätt att begära ut uppgifter. Regeringen har i 19 och 20 §§ förordningen (1999:1134) om belastningsregister meddelat föreskrifter om vilka myndigheter som får medges direktåtkomst. Liksom i fråga om passagerarregistret har möjligheten att medge direktåtkomst begränsats på så sätt att det endast är vissa av de myndigheter som har rätt att få ut uppgifter från registret som också får medges sådan åtkomst. Det saknas bestämmelser om elektroniska utlämnanden i annan form. Något uttryckligt förbud mot sådant utlämnande har alltså inte införts för detta register och inte heller andra begränsande regler. Frågan om andra elektroniska utlämnanden än genom direktåtkomst från registret på medium för automatiserad behandling berördes inte i förarbetena (prop. 1997/98:97).

I sammanhanget kan också nämnas förslaget till en ny domstolsdatalag som innehåller en bestämmelse som generellt medger utlämnanden till myndigheter i elektronisk form (18 §). I övrigt får personuppgifter i mål lämnas ut elektroniskt till part eller dennes ombud m.fl. och annars endast i fråga om enstaka personuppgifter. Som skäl anfördes bl.a. följande (Ds 2013:10 s. 125 f.). Det finns starka effektivitetsskäl som talar för att inte begränsa elektroniskt utlämnande till andra myndigheter, inklusive andra domstolar. Eftersom de integritetsrisker som förknippas med sådant utlämnande inte är påtagliga, föreslås inga särskilda begränsningar. När det däremot gällde utlämnanden till enskilda är integritetsriskerna inte obetydliga och utrymmet för s.k. massuttag borde begränsas. Det bör

emellertid överlämnas till regeringen eller den myndighet som regeringen bestämmer att medge att utlämnanden i elektronisk form får ske även i andra fall.

Andra bestämmelser som kan begränsa ett utlämnande av personuppgifter

Bestämmelser i personuppgiftslagen

När personuppgiftslagen är tillämplig krävs att en myndighet innan ett utlämnande av personuppgifter har konstaterat att utlämnandet är en tillåten behandling enligt lagen. Det gäller oavsett i vilken form uppgifterna lämnas ut och oavsett vem mottagaren av uppgifterna är. För det första behöver myndigheten ta ställning till om samtliga de grundläggande kraven i 9 § är uppfyllda. Därvid gäller som ett första krav enligt 9 § första stycket a att den personuppgiftsansvarige ska se till att personuppgifter behandlas bara om det är lagligt. Det är således inte tillräckligt att myndigheten bedömer att utlämnandet är förenligt med finalitetsprincipen i 9 § första stycket d, dvs. att mottagaren inte ska behandla uppgifterna för något ändamål som är oförenligt med det ändamål för vilket myndigheten en gång samlade in uppgifterna. Utlämnandet ska också vara en tillåten behandling enligt 10–22 §§.

Därutöver innebär bestämmelserna i 31 § ett allmänt krav på den personuppgiftsansvarige att vidta säkerhetsåtgärder för att skydda de personuppgifter som myndigheten behandlar. Dessa krav gäller alltså oavsett vilken behandling det är frågan om. Ett utlämnande i elektronisk form, exempelvis via e-post, kan innebära att det uppstår särskilda risker vid överföringen av personuppgifterna som behöver motverkas.

Om personuppgifter lämnas ut till en annan myndighet torde utgångspunkten vara att den mottagande myndigheten kan antas behandla uppgifterna för ett godtagbart ändamål om det kan konstateras att utlämnandet är förenligt med de sekretessbestämmelser som gäller för berörda myndighetsområden. Så kan exempelvis vara fallet om det finns en sekretessbrytande bestämmelse som medger utlämnandet. Om uppgifter lämnas ut med stöd av den s.k. generalklausulen i 10 kap. 27 § OSL, dvs. efter en intresseavvägning, torde det också stå klart att den mottagande myndigheten behöver

de uppgifter som begärs ut. Utlämnandet torde i så fall uppfylla kraven i 9 § första stycket f PuL om att inte fler uppgifter får behandlas än som är nödvändigt med hänsyn till ändamålet med behandlingen.

Om personuppgifter lämnas till en annan myndighet i andra fall, t.ex. om utlämnandet avser enbart offentliga uppgifter, kan man fråga sig vilka krav som ställs på den utlämnande myndigheten för att den ska kunna konstatera att det är fråga om en tillåten behandling enligt personuppgiftslagen. En verksamhet som bedrivs av en statlig eller kommunal myndighet är ju, till skillnad från vad som gäller i fråga om enskilda, reglerad på ett eller annat sätt. Man kan därmed fråga sig om det finns anledning för den utlämnande myndigheten att exempelvis bedöma om alla de uppgifter som begärs ut behövs hos den mottagande myndigheten eller försäkra sig om att den mottagande myndigheten på ett godtagbart sätt har t.ex. begränsat antalet handläggare som ska få behörighet att få ta del av uppgifterna eller att andra liknande säkerhetsåtgärder har vidtagits. Varken personuppgiftslagen eller dataskyddsdirektivet ger emellertid något uttryckligt svar på frågan om det är förenligt med det regelverket att tillämpa en presumtion för att utlämnanden till andra myndigheter, som inte hindras av sekretess, utgör en tillåten behandling enligt personuppgiftslagen.

I den händelse det är frågan om att lämna ut personuppgifter till enskilda på grund av rätten att ta del av allmänna handlingar enligt 2 kap. TF gäller inte personuppgiftslagens bestämmelser. Frågan om det finns hinder mot utlämnandet ska då enbart bedömas utifrån bestämmelserna om sekretess i offentlighets- och sekretesslagen. I det sammanhanget får den s.k. PuL-sekretessen i 21 kap. 7 § OSL en särskild betydelse. Den bestämmelsen behandlas i följande avsnitt.

Bestämmelsen om ”PuL-sekretess” i 21 kap. 7 § OSL

Enligt 21 kap. 7 § OSL gäller sekretess för personuppgift, om det kan antas att ett utlämnande skulle medföra att uppgiften behandlas i strid med personuppgiftslagen.

Även om paragrafens formulering är något oklar, får det anses fastslaget i praxis att den enbart tar sikte på mottagarens be-

handling av personuppgifter (se HFD 2014 ref. 66 med där gjorda hänvisningar). Det som ska bedömas enligt bestämmelsen är alltså endast huruvida mottagarens avsedda behandling av de personuppgifter som begärs ut uppfyller kraven enligt personuppgiftlagen. Den bedömningen bör inte enbart ta sikte på en prövning utifrån finalitetsprincipen i 9 § första stycket d PuL, utan på samtliga bestämmelser i lagen.

Om den utlämnande myndigheten blir varse eller självmant bedömer att det kan antas finnas sådana brister i mottagarens kommande behandling av de personuppgifter som avses lämnas ut att denna blir lagstridig, torde det i och för sig inte heller vara tillåtet enligt personuppgiftslagen att lämna ut uppgifterna. Att lämna ut personuppgifterna i en sådan situation, dvs. då det kan befaras att mottagaren inte kommer att uppfylla kraven på en tillåten behandling, skulle alltså inte heller vara en tillåten behandling för den utlämnande myndigheten i den mån personuppgiftslagen ska tillämpas på utlämnandet.

Enligt 21 kap. 7 § OSL gäller sekretess med ett rakt skaderekvisit. Det innebär ett relativt svagt sekretesskydd, dvs. det ska presumeras att sekretess inte hindrar att personuppgifterna lämnas ut. I princip torde det innebära att det ska presumeras att mottagaren av personuppgifterna kommer att behandla dem i enlighet med personuppgiftslagen. I anslutning till de lagstiftningsärenden som ligger till grund för bestämmelsen i dess nuvarande lydelse har frågan om valet av skaderekvisit emellertid inte behandlats (prop. 1997/98:44 s. 147 och prop. 2008/09:150 s. 340). Där finns således inga uttalanden om vad valet av skaderekvisit betyder för vad som kan krävas av en utlämnande myndighet när det gäller att pröva huruvida mottagarens behandling av de uppgifter som begärs ut kommer att omfattas av och vara förenlig med personuppgiftslagen. I förarbetena till motsvarande sekretessbestämmelse som gällde under datalagens tid, och som då enbart tog sikte på uttag ur regelrätta register, anfördes att en begäran om massuttag eller selekterade uppgifter alltid borde utgöra anledning för myndigheten att närmare utreda hur det är avsett att uppgifterna ska användas och att det är först om sökanden kan ange en godtagbar förklaring som uppgifterna bör lämnas ut (prop. 1973:33 s. 140).

Ett rakt skaderekvisit innebär typiskt sett att skadebedömningen ska kunna göras med utgångspunkt i själva uppgiften. Frågan om

sekretess gäller behöver därmed inte i första hand knytas till en skadebedömning i det enskilda fallet. Avgörande bör i stället vara om uppgiften är av den arten att ett utlämnande typiskt sett kan vara ägnat att medföra skada för det intresse som ska skyddas genom bestämmelsen. Om uppgiften i stället är sådan att den genomsnittligt måste betraktas som harmlös ska den alltså normalt falla utanför sekretesskyddet. En typiskt sett känslig uppgift omfattas däremot normalt av sekretess (Lenberg m.fl., inledande avsnitt 4.5.1). En typiskt sett harmlös uppgift kan emellertid skyddas av sekretess med ett rakt skaderekvisit om det exempelvis i ett särskilt fall framgår att den som begär att få ut en uppgift kan använda den för att utsätta den som uppgiften rör för trakasserier. Avsikten är emellertid inte att tjänstemännen vid myndigheterna normalt ska försöka ta reda på om det finns indikationer av nu nämnt slag.

I de fall det blir aktuellt att tillämpa sekretessbestämmelsen i 21 kap. 7 § OSL har det vanligen redan konstaterats att sekretess för uppgifterna inte gäller enligt någon annan bestämmelse i lagen. Den fråga som alltså normalt ska bedömas är om 21 kap. 7 § hindrar ett utlämnande av uppgifter som i övrigt är att anse som offentliga, dvs. som typiskt sett inte är i behov av skydd. Utgångspunkten är alltså att de aktuella uppgifterna i sig i allmänhet inte är av sådan art att sekretessen aktualiseras. Det ska i stället vara den avsedda behandlingen av uppgifterna hos mottagaren som kan föranleda ett sekretesskydd, dvs. att uppgifterna kommer att behandlas på ett sätt som strider mot personuppgiftslagen. Ett rakt skaderekvisit innebär emellertid, som påpekats ovan, att tjänstemännen vid myndigheterna normalt inte ska försöka ta reda på om det finns omständigheter som talar för att ett sekretesskydd behövs.

Praxis på området från Högsta förvaltningsdomstolen är sparsam. Domstolen har bl.a. i ett par avgöranden prövat om bestämmelsen utgör ett hinder mot att lämna ut personuppgifter från Jordbruksverket respektive Centrala studiestödsnämnden för kommersiella intressen, och fann efter en intresseavvägning enligt 10 § f PuL att utlämnandet inte hindrades av sekretess (RÅ 2001 ref. 68 resp. RÅ 2002 ref. 54). I det sistnämnda avgörandet var det fråga om privatpersoners uppgifter och då borde enligt domstolen mottagarens kommersiella intressen på ett entydigt sätt utfalla till dennes förmån i stället för den enskildes integritetsintressen för att

ett utlämnande skulle vara tillåtet. En utförlig redovisning för rättspraxis som rör tillämpning av 21 kap. 7 § OSL finns i Öman/Lindblom, s. 581 f.

Frågan om tillämpningen av 21 kap. 7 § OSL har också utförligt behandlats av E-offentlighetskommittén, som bl.a. hade till uppgift att överväga om bestämmelsen borde upphävas (SOU 2010:4 s. 317 f.). Kommittén fann att bestämmelsen fyllde i vart fall en viss begränsad funktion och därför inte borde upphävas. Vidare föreslog kommittén att bestämmelsen skulle förtydligas så att det inte råder någon tvekan om att det bara är sökandens efterföljande behandling som är relevant för den sekretessprövning som ska göras och inget annat. Förslaget har ännu inte lett till lagstiftning.

Bestämmelsen har föranlett kritik bl.a. av den anledningen att den tycks förutsätta att myndigheten skaffar sig en uppfattning om syftet med en begäran om utlämnande av allmänna handlingar eller uppgifter. JO har påpekat att den därför harmonierar mindre väl med efterfrågeförbudet i 2 kap. 14 § tredje stycket TF, dvs. den principiella rätten att anonymt få begära ut allmänna handlingar och därför borde ändras eller upphävas (se JO:s dnr 1102-2004 och 1849-2004). I sitt beslut den 28 augusti 2013 (dnr 4171-2011) utvecklade JO sin syn på hur efterfrågeförbudet kunde förenas med 21 kap. 7 § OSL. JO anförde bl.a. att det står klart att myndigheten inte får börja ställa frågor om sökandens tilltänkta användning bara för att en personuppgift begärs utlämnad. Enligt JO krävs det för det första att det finns någon konkret omständighet som gör att det kan antas att personuppgiften efter utlämnandet kommer att behandlas på ett sätt som omfattas av personuppgiftslagen. Sådana omständigheter kan – förutom de upplysningar som sökanden på eget initiativ kan ha lämnat om sin tilltänkta användning av uppgifterna – vara att sökanden begär ut uppgifter om väldigt många personer från ett register (ett s.k. massuttag) eller uppgifter om ett urval av personer med vissa karakteristika, t.ex. inkomst, språktillhörighet, politisk tillhörighet osv. (s.k. selekterade uppgifter). JO anförde att först om det på grund av någon konkret omständighet finns skäl att anta att sökanden kommer att behandla uppgifterna på ett sätt som omfattas av personuppgiftslagen, t.ex. för att begäran omfattar uppgifter om många personer, finns det anledning att genom frågor till sökanden försöka ta reda på hur och till vad sökanden ska använda uppgifterna för att kunna bedöma om den

tilltänkta behandlingen strider mot personuppgiftslagen. Myndigheten får dock enligt 2 kap. 14 § tredje stycket TF inte ställa mer inträngande eller fler frågor än som behövs för att göra en sekretessbedömning.

Regler om rutinmässigt utlämnande av personuppgifter till andra myndigheter

I registerförfattningar finns ofta bestämmelser som föreskriver att personuppgifter får tillhandahållas vissa särskilt angivna myndigheter. Sådana bestämmelser fanns redan före personuppgiftslagens tid, men återfinns efter den lagens införande ofta under rubriken ”Sekundära ändamål”. Dessa bestämmelser syftar i grunden till att styra huruvida uppgifter rutinmässigt får lämnas ut till en annan myndighet och inte till på vilket sätt uppgifter får lämnas ut. Frågan har emellertid ett samband med frågan om elektroniskt utlämnande på det sättet att om det finns behov av ett rutinmässigt uppgiftsutbyte, torde det utbytet kunna effektiviseras genom att utlämnandet av uppgifter sker elektroniskt.

Ett rutinmässigt utlämnande av uppgifter till en annan myndighet kan förstås regleras på så sätt att det införs en uppgiftsskyldighet mellan de myndigheter som ska utbyta information. Om någon uppgiftsskyldighet inte finns föreskriven kan ett rutinmässigt utlämnande av sekretessreglerade uppgifter i stället äga rum med stöd av den s.k. generalklausulen i 10 kap. 27 § OSL, dvs. efter en avvägning mellan intresset av att skydda uppgifterna hos den utlämnande myndigheten och intresset hos den mottagande myndigheten av att få ut uppgifterna. Om det är uppenbart att intresset av att uppgifterna lämnas ut har företräde, ska uppgifterna lämnas ut. Det följer av bestämmelserna i 6 kap. 5 § OSL om myndigheters skyldighet att lämna information till varandra.

Det krävs ingen särskild författningsreglering för att ett rutinmässigt utlämnande av personuppgifter till en annan myndighet ska kunna äga rum. Bestämmelserna i 10 kap. 27 § OSL bygger emellertid på att ett sådant utlämnande ska vara författningsreglerat (Lenberg m.fl., kommentaren till 10 kap. 27 §). Har det i en lag eller författning föreskrivits att uppgifter ”bör” eller ”får” lämnas ut får det antas att lagstiftaren har bedömt att intresset av att uppgifter lämnas mellan myndigheter har företräde framför sekretess-

intresset. Även om det inte är frågan om en sådan absolut uppgiftsskyldighet som avses i 10 kap. 28 §, torde det finnas ett relativt litet utrymme för den utlämnande myndigheten att i en konkret utlämnandesituation göra en annan bedömning.

I den händelse man har tänkt sig att ett rutinmässigt uppgiftsutbyte ska äga rum mellan myndigheter och det avser sekretessreglerade uppgifter, bör utgångspunkten alltså normalt vara att uppgiftsutbytet ska komma till uttryck i en lag eller förordning där det uttrycks att en myndighet ”bör” eller ”får” lämna ut uppgifter till en annan myndighet. För att återknyta till frågan om elektroniskt utlämnande kan man alltså konstatera att, även om man kommer till slutsatsen att det inte behöver regleras särskilt om ett utlämnande kan ske i elektronisk form, det ändå kan behövas en reglering för att uttrycka att ett rutinmässigt uppgiftsutbyte får komma till stånd. I den mån sådana bestämmelser införs, är det alltså vår uppfattning att lagstiftaren därmed har tagit ställning till att utlämnandet sker i enlighet med finalitetsprincipen, se avsnitt 9.2.4.

11.2.2 Terminologin rörande annat elektroniskt utlämnande

Bakgrund

I avsnitt 11.1.1 gör vi bedömningen att begreppet direktåtkomst även fortsättningsvis bör ges den innebörd som får anses vara den redan etablerade, dvs. att en direktåtkomst föreligger om en myndighet hos en annan myndighet har en sådan teknisk tillgång till upptagningar som avses i 2 kap. 3 § andra stycket TF. Vidare föreslås att det i den nya lagen om myndigheters behandling av personuppgifter införs en bestämmelse som innebär att direktåtkomst till sekretessreglerade uppgifter kräver ett uttryckligt stöd i lag eller förordning. Därutöver föreslår vi att det i 10 kap. 28 § OSL förs in ett nytt andra stycke, där det föreskrivs att bestämmelser i lag eller förordning som medger direktåtkomst i sig bryter sekretess. Den generellt sekretessbrytande bestämmelsen tar bara sikte på sådan åtkomst för myndigheter, inte för enskilda.

Sådana utlämnanden i elektronisk form som inte sker inom ramen för en direktåtkomst brukar vanligen betecknas utlämnanden på medium för automatiserad behandling. Till skillnad från direktåtkomst innebär de alltså inte att mottagaren bildligt tillåts att ”kliva

in” innanför myndighetens gränser för att där ta del av uppgifter, utan uppgifter både begärs ut av och levereras till en mottagare utanför myndigheten. Sådana utlämnanden kan också ske på den utlämnande myndighetens eget initiativ.

Till skillnad från de faktiska överföringar av uppgifter som äger rum inom ramen för en direktåtkomst, vilka rättsligt innebär att mottagaren själv gör dessa överföringar från den mängd av uppgifter som i tryckfrihetsförordningens mening alltså har lämnats ut i den stund åtkomsten etablerats, innebär andra former av elektroniska utlämnanden att uppgifter lämnas ut i det enskilda fallet endera på begäran av mottagaren eller på initiativ av den utlämnande myndigheten. I de fallen är alltså ett utlämnande av uppgifter en reaktion från den utlämnande myndighetens sida på en begäran från en mottagare eller ett resultat av dess egna beslut. Det kännetecknade för en direktåtkomst är däremot att det inte behövs att utlämnande myndighet reagerar på någon begäran från en mottagare eller fattar något eget beslut om utlämnande, eftersom mottagaren i rättslig mening redan har getts tillgång till uppgifterna.

Enligt 3 § PuL definieras behandling av personuppgifter som varje åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter, vare sig det sker på automatisk väg eller inte. Som exempel nämns utlämnande genom översändande, spridning eller annat tillhandahållande av åtgärder. I enlighet med denna terminologi torde ett ”annat elektroniskt utlämnande” närmast kunna beskrivas som en behandling av personuppgifter som innebär att uppgifterna lämnas ut genom att sändas över till mottagaren.

Våra överväganden

Bedömning: Begreppet utlämnande på medium för automatiserad behandling bör utmönstras. I stället bör begreppet utlämnande i elektronisk form användas, varmed avses alla andra elektroniska utlämnanden än direktåtkomst.

I dag förekommer det i registerförfattningar alltså ett antal olika begrepp för att beskriva sådant elektroniskt utlämnande som inte är direktåtkomst, se avsnitt 5.4. Ett vanligt förekommande begrepp är utlämnande på medium för automatiserad behandling. Enligt vår

uppfattning är det ett uttryck som framstår som väldigt otympligt. Det är emellertid klart att det som åsyftas är andra elektroniska utlämnanden än de som sker genom direktåtkomst. Om nu direktåtkomst ges en särskild reglering såväl i offentlighets- och sekretesslagen som i den nya lagen om myndigheters personuppgiftsbehandling och en viss definition av vad som avses med sådan åtkomst ges, ser vi inget hinder mot att i övrigt i rättsliga sammanhang övergå till att tala om utlämnanden i elektronisk form (se t.ex. E-offentlighetskommitténs förslag om ny skyldighet för myndigheter att lämna ut allmänna handlingar i sådan form i betänkandet SOU 2010:4). Om det i en författningstext rörande exempelvis rutinmässigt uppgiftsutbyte inte uttryckligen anges att det är fråga om direktåtkomst, skulle man därmed motsatsvis kunna dra slutsatsen att det som avses är någon annan form av elektroniskt utlämnande.

En nackdel med begreppet utlämnande i elektronisk form är att det inte alls rättsligt beskriver att med uttrycket avses ett annat utlämnande än det som sker genom direktåtkomst. Den beteckning som ofta används i dag – utlämnande på medium för automatiserad behandling – beskriver emellertid inte heller vad denna rättsliga åtskillnad består i. Rent tekniskt kan utlämnanden inom ramen för en direktåtkomst också göras genom något slags medium för automatiserad behandling, både då den tekniska åtkomsten etableras och därefter då de faktiska överföringarna av uppgifter äger rum. Det kan dock konstateras att utlämnande i elektronisk form är mer i överensstämmelse med modernt språkbruk än vad det hittills normalt använda begreppet är.

Vi föreslår därför att begreppet utlämnande på medium för automatiserad behandling inte längre ska användas utan att man i stället bör använda begreppet utlämnande i elektronisk form, varmed avses andra elektroniska utlämnanden än direktåtkomst. Det som avses är således samtliga andra fall då en myndighet lämnar ut uppgifter genom att elektroniskt på det ena eller andra sättet förmedla dem till mottagaren.

11.2.3 Bör utlämnande i elektronisk form kräva stöd i lag eller förordning?

Bakgrund

Vi har ovan i avsnitt 5.7 dragit slutsatsen att starka skäl talar för att det också i fortsättningen bör göras en åtskillnad mellan direktåtkomst å ena sidan och andra former av utlämnanden i elektronisk form å den andra. Därutöver har vi i samma avsnitt bedömt att det saknas behov av att göra en rättslig åtskillnad mellan olika andra former av utlämnanden i elektronisk form.

Det kan konstateras att många registerförfattningar innehåller bestämmelser som syftar till att begränsa aktuell myndighets möjlighet att lämna ut uppgifter och handlingar i elektronisk form, dvs. normalt genom regler om utlämnande på medium för automatiserad behandling. Ibland begränsar sådana bestämmelser endast utlämnanden till enskilda, men i vissa fall gäller begränsande regler både i förhållande till andra myndigheter och enskilda. En första fråga blir därför om det i en samlad lag för myndigheters behandling av personuppgifter bör finnas bestämmelser som ställer upp ett grundläggande krav på att utlämnande i elektronisk form ska ha stöd i författning för att vara tillåtet. En annan fråga blir därefter om det bör införas bestämmelser som generellt begränsar myndigheters möjlighet att lämna ut personuppgifter i elektronisk form, vilken behandlas i nästa avsnitt.

Våra överväganden

Bedömning: Det saknas skäl för att införa ett grundläggande krav på att utlämnanden av personuppgifter i elektronisk form ska ha stöd i författning för att vara tillåtet.

Som redan konstaterats måste en direktåtkomst som avses omfatta sekretessreglerade uppgifter hos den utlämnande myndigheten förenas med en sekretessbrytande regel. Ett utlämnande som inte innebär direktåtkomst aktualiserar i sig inte någon sådan fråga. Det frågan då handlar om är enbart valet av utlämnandeform. De frågor som aktualiseras inför utlämnandet, t.ex. om det finns hinder mot utlämnandet p.g.a. sekretess eller om en sekretessbrytande regel

kan tillämpas, är enkelt uttryckt redan avklarade i så måtto att de redan är reglerade. Det står m.a.o. klart i vilken mån ett utlämnande av personuppgifter alls kan ske, frågan är enbart i vilken form. I ett lagstiftarperspektiv väcker således ett utlämnande i elektronisk form, till skillnad från direktåtkomst, inte frågor om sekretess utan om andra frågor som har anknytning till själva valet av utlämnandeform. En sådan fråga är exempelvis om det finns andra regler om integritetsskydd än sekretessbestämmelser som styr eller bör styra valet av utlämnandeform och om det i så fall bör föranleda särskild reglering.

Ett utlämnande i elektronisk form, dvs. ett utlämnande som inte sker genom direktåtkomst, medför inte heller i sig att det uppstår krav på att vare sig den utlämnande eller mottagande myndigheten vidtar några särskilda säkerhets- eller kontrollåtgärder i förväg. En annan sak är dock att brister i möjligheten att säkert överföra personuppgifter elektroniskt eventuellt kan innebära att ett utlämnande i elektronisk form är olämpligt. Vi återkommer till den frågan nedan.

De frågor som väcks i samband med utlämnanden i elektronisk form är alltså av ett annat och mer allmänt slag än de som uppstår i samband med direktåtkomst.

Mot bakgrund av utformningen av gällande registerförfattningar torde den slutsatsen kunna dras att lagstiftaren hittills har gjort bedömningen att ett utlämnande på medium för automatiserad behandling inte i sig kräver författningsstöd för att vara tillåtet. Däremot har lagstiftaren gjort skilda bedömningar i olika lagstiftningsärenden när det gäller frågan om det i det aktuella fallet med hänsyn till framför allt intresset av integritetsskydd finns ett behov av att införa begränsningar mot ett sådant utlämnande mellan myndigheter.

Vi kan för vår del inte heller se att det vare sig med hänsyn till intresset för skydd av den enskildes integritet eller av annat skäl skulle finnas något behov av att införa ett grundläggande generellt krav på att en myndighets utlämnande av personuppgifter i elektronisk form ska ha stöd i författning för att vara tillåtet. Vi föreslår därför inte någon sådan regel.

11.2.4 Behövs en särskild bestämmelse som begränsar utlämnanden i elektronisk form?

Bakgrund

Att det i en registerförfattning inte har införts några särskilda begränsningar i möjligheterna att lämna ut personuppgifter i elektronisk form innebär inte att det är fritt fram att lämna ut uppgifter i sådan form. I lagstiftningsärendet om patientdata anfördes att det ankom på den utlämnande myndigheten att göra en lämplighetsprövning, varvid eventuella risker från säkerhets- och integritetssynpunkt skulle vägas mot intresset av ett effektivt utlämnande (prop. 2007/08:126 s. 77). Att man i det sammanhanget talar om en ”lämplighetsprövning” torde ha sin grund i den omständigheten att det på hälso- och sjukvårdsområdet inte finns någon skyldighet att lämna ut uppgifter i elektronisk form. Att myndigheter skulle ha en sådan skyldighet finns vanligtvis inte heller föreskrivet. Om ett utlämnande i elektronisk form varken hindras eller anbefalls av någon regel, står det alltså i allmänhet en myndighet fritt att avgöra om ett utlämnande ska ske i denna eller någon annan form utifrån vad myndigheten finner lämpligt.

Det är dock inte enbart i samband med en sådan ”lämplighetsprövning” som omtalas i förarbetena till patientdatalagen som en utlämnande myndighet kan behöva bedöma vilka risker från säkerhets- och integritetssynpunkt som ett utlämnande av personuppgifter kan ge upphov till. Innan det blir aktuellt att göra en sådan lämplighetsprövning, ska det ju stå klart att utlämnandet som sådant är en tillåten behandling enligt personuppgiftslagen, dvs. oavsett utlämnandeform. I det sammanhanget är det inte tillräckligt att konstatera att utlämnandet är förenligt med finalitetsprincipen, utan samtliga grundläggande krav i 9 § ska vara uppfyllda liksom övriga krav i lagen. Vid ett utlämnande som grundar sig på rätten att ta del av allmänna handlingar är det i stället 21 kap. 7 § OSL som kan utgöra hinder mot att personuppgifter lämnas ut, varvid det indirekt prövas om mottagarens avsedda behandling strider mot personuppgiftslagen.

Det kan alltså konstateras att det finns ett författningsreglerat krav på den utlämnande myndigheten att enligt antingen bestämmelserna i personuppgiftslagen eller sekretessregeln i 21 kap. 7 § OSL ta ställning till om ett utlämnande av personuppgifter är tillåtet.

Detta krav gäller oavsett i vilken form utlämnandet sker. När det har konstaterats att ett utlämnande är tillåtet, återstår alltså att avgöra i vilken form utlämnandet bör ske. Eftersom det står myndigheten fritt att avgöra detta, om inga särskilda begränsningar finns, blir det fråga om en lämplighetsprövning.

Våra överväganden och förslag

Förslag och bedömning: Det behöver inte införas någon bestämmelse som generellt begränsar myndigheters möjlighet att lämna ut personuppgifter till andra myndigheter i elektronisk form.

När det gäller utlämnanden till enskilda föreslås en bestämmelse i den nya lagen som föreskriver att om en personuppgift får lämnas ut till en enskild, kan det ske i elektronisk form om det inte är olämpligt med hänsyn till skyddet för personuppgiften. Därmed erinras myndigheterna om att det ankommer på dem att först göra en prövning av om ett utlämnande, oavsett form, av personuppgifter är tillåtet. Om så är fallet, är utgångspunkten att det kan ske i elektronisk form. En sådan bestämmelse leder till en mer nyanserad bedömning när det gäller skyddet för enskildas integritet än vad som följer av sådana regler som i dag är vanliga i registerförfattningar och som begränsar elektroniskt utlämnande till enskilda.

Utlämnanden till andra myndigheter

I flera av de lagstiftningsärenden där man bedömt att det behövs bestämmelser som begränsar utlämnanden i elektronisk form i en viss myndighets verksamhet synes man ha ansett att den avgörande frågan för om det behövs särskilda begränsningar mot ett utlämnande av personuppgifter i elektronisk form är om det kan antas finnas en risk för att den mottagande myndigheten kommer att behandla uppgifterna för ett ändamål som inte är avsett, dvs. att det finns risk för att uppgifterna kan komma att behandlas i strid med finalitetsprincipen och eventuellt även i strid med andra bestämmelser som syftar till att skydda personuppgifter hos den myndigheten.

I princip är det givetvis så att även ett utlämnande av personuppgifter till en annan myndighet måste, i likhet med sådana utlämnanden till enskilda, vara tillåtet enligt bestämmelser om sekretess och enligt personuppgiftslagen. Vidare bör ett utlämnande som i och för sig är tillåtet inte ske i elektronisk form om detta i något beaktansvärt hänseende skulle vara olämpligt. Frågan är emellertid hur långtgående en myndighets prövning av lagenlighet och lämplighet behöver vara när det rör sig om ett uppgiftsutbyte med en annan myndighet. Den frågan har i sin tur betydelse för vilken utgångspunkt det är motiverat för lagstiftaren att ha när det gäller frågan om det finns anledning att begränsa en myndighets möjlighet att lämna ut personuppgifter till en annan myndighet i elektronisk form.

Vi har ovan konstaterat att såvitt avser utlämnande av personuppgifter till enskild detta kan ske endera i form av ett uttag enligt offentlighetsprincipen eller på annan grund, t.ex. vid försäljning av uppgifter. Vi har också konstaterat att prövningen inte ska ske mot personuppgiftslagen utan uteslutande mot offentlighets- och sekretesslagen vid ett uttag med stöd av 2 kap. TF. Principiellt sett föreligger den skillnaden att vid ett offentlighetsuttag personuppgiftslagen inte är tillämplig på den personuppgiftsbehandling som myndighetens utlämnande innebär. Prövningen tar då enbart sikte på mottagarens tänkta kommande behandling av personuppgifterna. När det gäller utlämnande mellan myndigheter ställer sig saken annorlunda. Myndigheter kan inte åberopa rätten till handlingsoffentlighet och sekretess gäller ju även mellan myndigheter. Vid utlämnande till en annan myndighet är personuppgiftslagen alltså tillämplig på själva utlämnandet men bestämmelsen i 21 kap. 7 § OSL gäller samtidigt också. Frågan blir därmed vilket betraktelsesätt som bör anläggas.

Offentlighets- och sekretesskommittén, som föreslog att det skulle införas en bestämmelse i 2 § PuL om att utlämnanden av uppgifter mellan myndigheter som sker i överensstämmelse med sekretessbestämmelser inte hindrades av personuppgiftslagen, påpekade att dåvarande 7 kap. 16 § sekretesslagen (nuvarande 21 kap. 7 § OSL) även är tillämplig mellan myndigheter. Enligt kommittén måste en utgångspunkt dock vara att en myndighet avser att följa lagen (SOU 2003:99 s. 236).

Enligt vår uppfattning är det rimligt att anlägga samma synsätt som Offentlighets- och sekretesskommittén när det gäller ett uppgiftsutbyte mellan myndigheter. En myndighet bör vid ett utlämnande till en annan myndighet alltså kunna utgå från att den mottagande myndigheten själv tar ansvar för att den exempelvis inte begär ut fler uppgifter än den behöver för att utföra den avsedda behandlingen samt att den har organiserat sin informationshantering så att personuppgiftslagens krav uppfylls, också i fråga om säkerhet. Den utlämnande myndighetens ansvar bör därmed som huvudregel kunna begränsas till att bedöma om det finns hinder mot utlämnandet på grund av någon annan sekretessbestämmelse än 21 kap. 7 § OSL. En prövning enligt 21 kap. 7 § skulle då bara behöva aktualiseras undantagsvis, närmast i uppenbara fall av förmodad lagstridighet. Frånsett sådana rena undantagsfall skulle det därmed inte finnas anledning för myndigheten att anse att det finns hinder mot ett utlämnande enligt offentlighets- och sekretesslagen och personuppgiftslagen. Det sagda innebär alltså en slags presumtion för att ett utlämnande av personuppgifter till en annan myndighet, som inte hindras av att sekretess gäller för uppgifterna i sig, inte innebär någon risk för kränkningar av enskildas integritet. Enligt vår uppfattning lämnar såväl dataskyddsdirektivet som förslaget till en uppgiftsskyddsförordning utrymme för att tillämpa en sådan presumtion. Vi menar alltså att man vid utlämnande av personuppgifter mellan myndigheter som sker i överensstämmelse med sekretessbestämmelser kan presumera att utlämnandet är lagenligt.

I enlighet med det synsättet saknas det enligt vår bedömning skäl att genom en generell bestämmelse begränsa myndigheters utlämnande av personuppgifter i elektronisk form till andra myndigheter. Från integritetsskyddssynpunkt finns det alltså ingen anledning att när det gäller utlämnanden till andra myndigheter generellt begränsa möjligheten att lämna ut personuppgifter elektroniskt. Det kan däremot eventuellt finnas andra skäl än integritetshänsyn som talar för att det för vissa myndigheters del skulle vara olämpligt att använda sig av ett elektroniskt utlämnande, t.ex. att det finns tekniska hinder och därför är opraktiskt. Sådana skäl kan dock knappast motivera införandet av en generell begränsning i fråga om möjligheterna att lämna ut personuppgifter i elektronisk form till

andra myndigheter. Vi föreslår därför inte att det införs någon sådan bestämmelse i den nya lagen.

En helt annan sak är att det ändå kan behövas särskilda regler som medger ett uppgiftsutbyte mellan vissa myndigheter så att lagstiftaren därigenom tar ställning till att ett rutinmässigt uppgiftsutbyte får komma till stånd. Det utgör i så fall en stark presumtion för att den s.k. generalklausulen i 10 kap. 27 § OSL medger ett utlämnande av sekretessreglerade uppgifter.

Utlämnande till enskilda

När det gäller utlämnanden av personuppgifter till enskilda kan en utlämnande myndighet knappast på motsvarande sätt som i förhållande till andra myndigheter tillämpa en presumtion för att det inte uppstår en risk för enskildas integritet. Visserligen omfattas även enskildas behandling av personuppgifter av personuppgiftslagen och Datainspektionens tillsyn och utlämnanden till enskilda kan avse sådana aktörer vars verksamhet står under statlig tillsyn även av annat slag, exempelvis försäkringsbolag och kreditmarknadsinstitut. Det går dock inte att komma ifrån att enskildas hantering av personuppgifter inte sker i en sådan i övrigt reglerad verksamhet som den statliga och kommunala förvaltningen utgör och inte heller är föremål för samma möjligheter till insyn och ansvarsutkrävande. Det är alltså ett ofrånkomligt faktum att då ett utlämnande av personuppgifter sker från en myndighet till en enskild, personuppgifterna lämnar en reglerad verksamhet för att hamna i en miljö som är relativt oreglerad.

Det kan alltså sägas uppstå ett slags spänningsfält för integritetsskyddet mellan myndighetens och den enskildes hantering av de personuppgifter som lämnas ut. Som befintlig lagstiftning är utformad är det i första hand bestämmelsen i 21 kap. 7 § OSL som ska tillämpas för att lösa sådana spänningar då det gäller utlämnanden av personuppgifter till enskilda. Om det är fråga om ett utlämnande på grund av 2 kap. TF är det vidare endast den bestämmelsen, frånsett givetvis övriga sekretessbestämmelser, som kan hindra ett utlämnande.

Som redan framgått har 21 kap. 7 § OSL vållat svårigheter i tillämpningen och det har t.o.m. funnits tankar på att helt upphäva

bestämmelsen. Den ger emellertid, tillsammans med den praxis som hittills bildats, en viss anvisning om vilken slags prövning som det ankommer på den utlämnande myndigheten att göra och när en sådan prövning aktualiseras. För det första kan det inte anses ankomma på den utlämnande myndigheten att vid varje utlämnande av personuppgifter till enskilda ha betänkligheter inför mottagarens behandling av uppgifterna, utan det ska finnas en särskild anledning att utreda vilken behandling som är avsedd och om den kan antas strida mot personuppgiftslagens bestämmelser. Att en stor mängd uppgifter begärs ut kan vara en sådan anledning (jfr RÅ 2002 ref. 54). I så fall bör det prövas om den enskilde har ett från integritetsskyddsperspektiv berättigat intresse av att få göra den avsedda behandlingen av personuppgifterna och att personuppgifterna är nödvändiga för den behandlingen, exempelvis att använda dem för marknadsföringsändamål. Om det inte är frågan om något av de fall av tillåten behandling som särskilt pekas ut i 10 § PuL, behöver en intresseavvägning göras. Om det är frågan om privatpersoners uppgifter och inte näringsidkares, bör enligt praxis mottagarens intresse av att få göra sin behandling på ett entydigt sätt väga över privatpersonernas intresse av skydd för sin integritet. Vari den enskildes behov av skydd består vid den tänkta behandlingen bör konkretiseras vid prövningen, t.ex. i fråga om hur känsliga uppgifterna är, om och hur mottagaren tänkt sprida uppgifterna och vilka anspråk den enskilde kan göra gällande gentemot den som avser att göra den aktuella behandlingen. Därefter kan en intresseavvägning göras. Om mottagarens i och för sig berättigade intresse av att få göra sin behandling inte kan anses väga över den enskildes intresse av skydd för sin integritet, exempelvis därför att mottagaren har tänkt sig att sprida uppgifterna på ett sådant sätt eller i sådan omfattning att detta blir oproportionerligt i förhållande till den enskildes behov av skydd, ska ett utlämnande inte ske.

Det kan alltså konstateras att många integritetsskyddsaspekter kan beaktas vid en prövning enligt 21 kap. 7 § OSL. Den frågan kan emellertid ställas om det finns ytterligare omständigheter av betydelse för den enskildes behov av skydd för den personliga integriteten som bör fångas upp genom en bestämmelse som generellt begränsar en myndighets möjlighet att lämna ut personuppgifter i elektronisk form till enskilda.

Av redogörelsen ovan framgår att det är vanligt att registerförfattningar begränsar möjligheterna att lämna ut personuppgifter till enskilda i elektronisk form, även om ett motsvarande utlämnande till myndigheter inte har begränsats. Patientdatalagen avviker därvid från de övriga exemplen eftersom den varken innehåller någon begränsning för andra myndigheter eller enskilda. På hälso- och sjukvårdsområdet gäller dock en stark sekretess som i allmänhet förhindrar att patientuppgifter över huvud taget lämnas ut.

E-offentlighetskommittén föreslog att det skulle införas en bestämmelse i 6 kap. OSL som föreskriver att en myndighet på begäran ska lämna ut en handling i elektronisk form om den inte innehåller sekretessbelagda uppgifter, det finns förbud i lag eller förordning mot sådant utlämnande eller det annars är olämpligt. Syftet med bestämmelsen var bl.a. att skapa en väsentligt ökad medvetenhet om att det är fullt möjligt att lämna ut handlingar i elektronisk form och att göra klart att en sökande inte kan anses avstå från rätten att få ut handlingar med stöd av 2 kap. TF bara genom en begäran om att få ut dem i elektronisk form (SOU 2010:4 s. 307). Vidare skulle en sådan bestämmelse innebära att alla organ som omfattas av offentlighetsprincipen, dvs. inte endast statliga myndigheter utan även kommuner och landsting, kommunala bolag m.fl., skulle ha att tillämpa den.

Kommitténs förslag hade sin grund i att myndigheterna, bl.a. p.g.a. osäkerhet om vilka möjligheter som gällande regelverk egentligen ger i fråga om att lämna ut handlingar med personuppgifter i elektronisk form, i onödan avstod från elektroniskt utlämnande.

Vår genomgång av registerförfattningarna ger inte anledning att göra någon annan bedömning än den kommittén gjorde. Enligt vår bedömning kan det vidare knappast sägas att registerförfattningarna i alltför stor utsträckning skulle sakna bestämmelser som syftar till att begränsa elektroniskt utlämnande av personuppgifter till enskilda och att det därför sker elektroniska utlämnanden i en omfattning som innebär risker för enskildas integritet, snarare tvärtom.

Av redovisningen ovan av de bestämmelser i personuppgiftslagen och offentlighets- och sekretesslagen som behöver tillämpas för att bedöma om ett utlämnande av personuppgifter över huvud taget är tillåtet framgår att dessa bestämmelser innebär att ett utlämnande inte får ske om det kan antas att personuppgifter inte kommer att behandlas i enlighet med personuppgiftslagen. Ett ut-

lämnande som innebär risker för lagstridig behandling av personuppgifter är alltså inte tillåtet och detta gäller oavsett om det sker i pappersform eller elektroniskt. Ändå är det ofta risker för den enskildes integritet som anförs som motiv för att införa bestämmelser som begränsar möjligheterna att lämna ut personuppgifter elektroniskt. En regel som, i enlighet med t.ex. 13 § studiestödsdatalagen, begränsar ett sådant utlämnande till enstaka uppgifter i enskilda fall syftar exempelvis till att hindra massuttag av personuppgifter. Ett massuttag av personuppgifter utgör dock enligt vår mening skäl för att göra en prövning enligt 21 kap. 7 § OSL och visar det sig då att det kan antas att mottagaren kommer att behandla uppgifterna i strid med personuppgiftslagen är inte heller ett utlämnande på papper tillåtet. I detta sammanhang bör framhållas att ett massuttag alltså kan aktualisera en prövning enligt 21 kap. 7 § OSL, men utgör inte i sig en indikation på att personuppgifter kommer att behandlas i strid med personuppgiftslagen. Flertalet av de massuttag av offentliga uppgifter som sker hos myndigheterna görs för berättigade ändamål och utan att det uppstår risker för enskildas integritet.

Att det är vanligt med bestämmelser om elektroniskt utlämnande i registerförfattningar tycks snarare bero på att sådana bestämmelser genom sin mer definitiva utformning är relativt enkla att tillämpa. Det går inte att komma ifrån att de överväganden som behöver göras med utgångspunkt i personuppgiftslagen och offentlighets- och sekretesslagen tar resurser i anspråk i form av kunskap och tid. Därtill kan de allmänna övervägandena kring vad som är lämpligt i det enskilda fallet, vilket kan handla om annat än integritetsskydd, också vara resurskrävande. Ur myndighetens synvinkel kan det därför tyckas vara effektivt med en begränsande regel. Det problematiska med detta är emellertid att för att myndigheten dessförinnan ska kunna konstatera att ett utlämnande över huvud taget är tillåtet behöver den ändå göra en prövning enligt personuppgiftslagen och/eller offentlighets- och sekretesslagen. Den prövningen kommer myndigheten alltså inte ifrån oavsett på vilket sätt personuppgifterna avses lämnas ut. Det finns således en risk med regler som begränsar ett utlämnande i elektronisk form, eftersom de kan uppfattas av myndigheterna så att ett utlämnande av personuppgifter är tillåtet om det är förenligt med en sådan regel, exempelvis avser enskilda uppgifter och det är i ett enskilt fall som

utlämnandet sker. I ett sådant fall kommer således den prövning av risken för kränkning av enskildas integritet som alltid ska göras inte att ske. Även ett sådant utlämnande kan vara i strid med personuppgiftslagen och/eller 21 kap. 7 § OSL, exempelvis om det är så att mottagaren samlar in enstaka uppgifter för att bygga upp en databas med personuppgifter om lagöverträdelser som innefattar brott, vilket enligt 21 § PuL som huvudregel är förbjudet för andra än myndigheter.

Enligt vår bedömning finns därför inte några bärande skäl som tar sikte på skyddet för personuppgifter som motiverar att det införs en bestämmelse som generellt begränsar en myndighets möjligheter att lämna ut sådana uppgifter till enskilda i elektronisk form. Det kan alltså inte bli frågan om att exempelvis föreslå en bestämmelse som innebär att det endast skulle vara möjligt att lämna ut personuppgifter i elektronisk form bara i de fall då enstaka personuppgifter lämnas ut i enskilda fall. Dessutom kan det starkt ifrågasättas om en sådan begränsning skulle vara förenlig med PSI-direktivet. Det saknas vidare skäl att på så sätt onödigtvis hindra att personuppgifter lämnas ut till en mottagare som inte kan antas komma att behandla dem i strid med personuppgiftslagen.

Skälen till att myndigheter väljer att inte lämna ut handlingar i elektronisk form, trots att det är tillåtet, torde många gånger handla om annat än hänsyn till enskildas integritet. Det kan exempelvis vara frågan om praktiska faktorer som talar emot att ett sådant utlämnande är lämpligt eller att det finns ekonomiska aspekter som handlar om resursbrist eller risk för minskade avgiftsintäkter (se SOU 2010:4 s. 312 f. och SOU 2014:10 s. 82). Det är alltså frågan om lämplighetsaspekter som inte tar sikte på att utlämnandet avser personuppgifter, utan hänför sig till att det allmänt sett inte är lämpligt i ett visst fall att använda sig av elektroniskt utlämnande. Att ha en bestämmelse som tar sikte på den typen av avvägningar framstår emellertid inte som motiverat i en lag om myndigheters behandling av personuppgifter, eftersom en sådan lag enbart har till syfte att skydda personuppgifter. En bestämmelse av det slaget hör snarare hemma bland föreskrifter som mer allmänt syftar till att ange en nivå för myndigheters serviceskyldighet. Av redovisningen ovan framgår att en sådan bestämmelse redan finns för domstolar och de statliga förvaltningsmyndigheterna genom bestämmelsen i 10 § serviceförordningen. För kommunernas del saknas emellertid

en sådan bestämmelse. Såsom utredningens uppdrag är formulerat saknas det vidare anledning att i detta sammanhang gå närmare in på den särskilda problematik som hänför sig till intäkter i samband med försäljning av information. Vad gäller denna fråga hänvisar vi i stället till den utförliga redovisning som finns i E-offentlighetskommitténs betänkande (SOU 2010:4 s. 167 f. och 343 f.).

Vad som enligt vår mening förtjänar att övervägas är om det bör införas en generell bestämmelse som inte i sak syftar till att begränsa ett elektroniskt utlämnande till enskilda men som erinrar om att det ankommer på myndigheterna att göra en prövning av dels om utlämnandet som sådant är tillåtet, dels om det i så fall är olämpligt att det sker i elektronisk form. En sådan bestämmelse skulle alltså ha som utgångspunkt att personuppgifter som får lämnas ut också kan lämnas ut i elektronisk form om mottagaren vill att personuppgifterna förmedlas på så sätt. Innan myndigheten förmedlar uppgifterna på detta sätt måste den emellertid först ta ställning till att det inte är ett olämpligt sätt att lämna ut uppgifterna. De lämplighetsaspekter som bestämmelsen tar sikte på bör avse sådana faktorer som har samband med integritetsskyddet och som inte direkt fångas upp av vare sig den nya lagen eller offentlighets- och sekretesslagen, exempelvis informationssäkerhetsfrågor. Vid ett utlämnande till enskilda som grundar sig på rätten att ta del av allmänna handlingar enligt 2 kap. TF kan det exempelvis handla om att myndigheten för egen del inte har ett informationssystem som på ett säkert sätt kan förmedla personuppgifter elektroniskt eller att ett elektroniskt utlämnande av något annat skäl medför att myndigheten inte på ett tillfredsställande sätt kan tillvarata skyddet för sina övriga personuppgifter till skillnad från om uppgifterna lämnas ut på papper. Det kan också handla om att en viss begärd utlämnandeform – t.ex. via okrypterad e-post – inte är lämplig alls medan en annan metod för förmedling i elektronisk form kanske vore fullt godtagbar. Enligt vår uppfattning kan en sådan bestämmelse leda till att myndigheter gör en mer nyanserad bedömning när det gäller skyddet för enskildas integritet än vad en tillämpning av de begränsande regler som i dag är vanliga i registerförfattningar leder till. Vi föreslår därför att det införs en bestämmelse som föreskriver att om en personuppgift får lämnas ut till en enskild, kan det ske i elektronisk form om det inte är olämpligt med hänsyn till skyddet för personuppgiften.

Vi vill avslutningsvis framhålla att det enligt vår bedömning alltjämt finns ett behov av att se över 21 kap. 7 § OSL i syfte att ge bestämmelsen en utformning som på ett bättre sätt än i dag ger myndigheterna ledning i hur bestämmelsen bör tillämpas vid ett utlämnande av annars offentliga personuppgifter samt ger personuppgifterna det skydd som ur ett dataskyddsrättsligt perspektiv kan behövas utöver vad som annars följer av offentlighets- och sekretesslagen. E-offentlighetskommittén har påpekat flera problem med bestämmelsen och dess konstruktion (se SOU 2010:4 s. 329). HFD 2014 ref. 66 aktualiserar vidare ånyo frågan om att 21 kap. 7 § OSL genom sin nuvarande utformning inte kan tillämpas vid utlämnanden av personuppgifter till en mottagare i utlandet. Eftersom 21 kap. 7 § OSL ska tillämpas oavsett i vilken form personuppgifter lämnas ut och alltså inte har någon direkt koppling till utlämnanden i elektronisk form, utgör behovet av en översyn emellertid inget hinder mot att införa den bestämmelse om sådana utlämnanden till enskilda som vi nu föreslår.

11.3 Bör sökbegränsningar som tar sikte på en utlämnande myndighet även gälla för en mottagande myndighet som har direktåtkomst?

11.3.1 Bakgrund

Uppdraget

I våra direktiv påpekas att ett absolut sökförbud i en registerförfattning även utgör en begränsning av vad som utgör en allmän handling enligt 2 kap. 3 § tredje stycket TF. Det är omdiskuterat vilken betydelse sökförbud i den utlämnande myndighetens registerförfattning har för bedömningen av frågan vilka sammanställningar av personuppgifter som utgör allmänna handlingar hos den mottagande myndigheten. I utredningens uppdrag ingår att ta ställning till vad som bör gälla i detta avseende.

Begränsningsregeln i 2 kap. 3 § TF

Enligt 2 kap. 3 § tredje stycket TF anses en sammanställning av uppgifter ur en upptagning för automatiserad behandling inte förvarad hos myndigheten om sammanställningen innehåller personuppgifter och myndigheten enligt lag eller förordning saknar befogenhet att göra sammanställningen tillgänglig.

Syftet med begränsningsregeln är att allmänheten inte med stöd av offentlighetsprincipen ska kunna ta del av sammanställningar av uppgifter ur upptagningar, dvs. s.k. potentiella handlingar, som myndigheten av hänsyn till skyddet för enskildas integritet själv är förhindrad att ta fram i sin egen verksamhet (prop. 2001/02:70 s. 23). Skyldigheten att ta fram sådana sammanställningar följer av 2 kap. 3 § andra stycket TF. Begränsningsregeln gällde även under datalagens tid, men fick en ny utformning i samband med grundlagsändringar år 2002 för att bl.a. anpassas till att personuppgiftslagen hade ersatt datalagen.

Begränsningsregeln omfattar inte s.k. färdiga elektroniska handlingar. Sådana handlingar anses alltid som förvarade hos en myndighet även om de innehåller personuppgifter och det i lag eller förordning finns förbud för myndigheten att använda vissa sökbegrepp vid sökningen efter handlingarna (a. prop. s. 38). Med begreppet personuppgift avses detsamma som i personuppgiftslagen med den skillnaden att begreppet enligt tryckfrihetsförordningen också omfattar avlidna personer.

Problembeskrivning i tidigare lagstiftningsarbeten

Informationsutbytesutredningen

Informationsutbytesutredningen behandlade frågan om vilka sökbegränsningar som gäller för mottagande myndighet i sitt betänkande Utökat elektroniskt informationsutbyte (SOU 2007:45). Enligt utredningen borde ledning hämtas från begränsningsregeln i 2 kap. 3 § tredje stycket TF (s. 198 f.). Om de sökbegränsningar som enligt lag eller förordning gäller för den myndighet som för databasen, dvs. för utlämnande myndighet, inte skulle gälla för annan myndighet som har direktåtkomst till uppgifter i databasen, skulle mottagande myndighet vid direktåtkomst få tillgång till samman-

ställningar av uppgifter som enligt 2 kap. 3 § TF inte anses förvarade hos utlämnande myndighet. Mottagande myndighet skulle därmed ha rätt att ta del av handlingar som inte är att anse som allmänna handlingar. Vidare skulle allmänheten kunna vända sig till mottagande myndighet och begära sammanställningar av uppgifter hos utlämnande myndighet som sistnämnda myndighet själv inte lagligen kan göra tillgängliga. En sådan tolkning av rättsläget var enligt Informationsutbytesutredningen inte rimlig och kunde inte ha varit lagstiftarens mening. Utredningen anförde att det ligger i sakens natur att en myndighet som ges direktåtkomst till uppgifter hos en annan myndighet aldrig kan ha vidare sökmöjligheter än utlämnande myndighet eller ta del av sammanställningar av uppgifter som inte anses förvarade hos utlämnande myndighet. Enligt utredningen måste bestämmelser om sökbegrepp i lagar och förordningar som tillämpas vid behandling av personuppgifter i viss angiven verksamhet därför utan särskild reglering gälla vid annan myndighets direktåtkomst till uppgifterna. Utredningens slutsats var därför att direktåtkomst i detta avseende inte innebär att tillgängligheten till uppgifter hos den utlämnande myndigheten ökar.

Vid remissbehandlingen av utredningens betänkande efterlystes en närmare analys av frågan. Den berördes emellertid inte i det fortsatta lagstiftningsarbetet med anledning av utredningens förslag (prop. 2007/08:160 s. 66 f. och 2008/09:KU2).

Vårt delbetänkande

I vårt delbetänkande konstaterade vi att det ingår i utredningens uppdrag att ta ställning i den aktuella frågan och att vi avsåg att återkomma till den i slutbetänkandet (SOU 2012:90 s. 116). Därutöver konstaterade vi att det inte råder någon tvekan om att en mottagande myndighet är skyldig att enligt 2 kap. 3 § andra stycket TF göra en sammanställning av tillgängliga personuppgifter, dvs. en s.k. potentiell handling, trots att den myndigheten i sin verksamhet inte får använda sig av direktåtkomst till den utlämnande myndighetens personuppgifter enligt en villkorad sökbegränsning eller s.k. ändamålsbegränsning i en registerförfattning. Den typen av begränsningar anses alltså inte utgöra sådana sökbegränsningar som avses enligt begränsningsregeln i 2 kap. 3 § tredje stycket TF. Frågan om

mottagande myndighet är bunden av de sökbegränsningar som gäller för utlämnande myndighet behandlades också i vårt resonemang om huruvida begränsningsregeln i 2 kap. 3 § tredje stycket TF borde ändras för att åtgärda problemen med s.k. överskottsinformation (a. bet. s. 152 f.). De frågeställningar som där tas upp behandlas också delvis i det följande.

Några exempel på hur frågan har reglerats

En förutsättning för att föreskrifter om sökbegränsningar som gäller sökning i en viss informationssamling hos en myndighet ska gälla för en annan myndighet som har direktåtkomst till uppgifter i den informationssamlingen är att föreskrifterna också ska tillämpas av den mottagande myndigheten. Registerförfattningar är emellertid vanligen endast tillämpliga i en viss myndighets verksamhet. Exempelvis gäller enligt 1 § lagen (2001:181) om behandling av uppgifter i Skatteverkets beskattningsverksamhet den lagen endast vid behandling av personuppgifter i Skatteverkets beskattningsverksamhet och i verkets handläggning av vissa borgenärsuppgifter. I 2 kap. 10 § andra och tredje styckena samma lag finns bestämmelser som begränsar vilka uppgifter som får användas som sökbegrepp vid sökning i beskattningsdatabasen, vilka enbart tar sikte på Skatteverkets verksamhet. Dessa sökbegränsningar gäller alltså inte för de myndigheter som enligt 2 kap. 7–8 a § får medges direktåtkomst till databasen. Enligt 7 § får exempelvis Skatteverket i dess medverkan i brottsutredningar medges sådan åtkomst. Bestämmelsen tar sikte på skattebrottsenheterna vars verksamhet utgör en självständig verksamhetsgren inom Skatteverket. I 14 a § lagen (1999:90) om behandling av personuppgifter i Skatteverkets medverkan i brottsutredningar finns särskilda sökbegränsningar som avser den sökning i beskattningsdatabasen som kan äga rum inom ramen för direktåtkomsten. Bestämmelsen infördes samtidigt som skattebrottsenheterna medgavs direktåtkomst till beskattningsdatabasen. När det gällde utformningen av författningsregleringen anförde regeringen att Skatteverkets möjligheter att använda sig av direktåtkomsten i den brottsbekämpande verksamheten skulle begränsas genom dels bestämmelser i lagen om Skatteverkets behandling av personuppgifter vid verkets medverkan i brottsutredningar, dels

personuppgiftslagen (prop. 2005/06:169 s. 85 f.). Bland annat skulle en begränsning införas när det gällde sökmöjligheter i fråga om fysiska personer. Det är alltså den som återfinns i den nämnda 14 a §.

I sammanhanget kan nämnas att i den tidigare skattegisterlagen (1980:343) användes en annan lagstiftningsteknik. I den lagen reglerades hur de dåvarande skatteregistren fick användas och inte specifikt för vilken myndighet som lagen som sådan gällde. I lagen föreskrevs vilka myndigheter som fick ha terminalåtkomst till registren. De begränsningar i fråga om sökbegrepp som gällde beträffande de olika registren gällde därför för alla de myndigheter som medgetts terminalåtkomst.

Enligt 114 kap. 2 § SFB gäller det kapitlet vid behandling av personuppgifter i verksamhet som gäller förmåner enligt balken, samt andra förmåner och ersättningar som enligt lag eller förordning eller särskilt beslut av regeringen handläggs av Försäkringskassan eller Pensionsmyndigheten. De begränsningar i fråga om sökbegrepp som föreskrivs i 27 § gäller således inte vid exempelvis den direktåtkomst som Centrala studiestödsnämnden (CSN) kan medges enligt 21 § och som får användas för att skapa underlag för beslut om och kontroll av förmåner m.m. i den verksamhet som nämnden bedriver. I studiestödsdatalagen (2009:287), som ska tillämpas vid behandling av personuppgifter i CNS:s studiestödverksamhet, finns i 8 § föreskrifter som generellt begränsar myndighetens användning av sökbegrepp vid dess behandling av personuppgifter. Dessa föreskrifter torde därför även begränsa vilka uppgifter som kan användas som sökbegrepp vid CSN:s användning av sin direktåtkomst till socialförsäkringsdatabasen.

I studiestödsdatalagen har alltså använts en delvis annan lagstiftningsteknik. Enligt 1 § tillämpas lagen vid behandling av personuppgifter i CSN:s studiestödsverksamhet. I 10 § föreskrivs att direktåtkomst eller annat elektroniskt utlämnande utan den registrerades samtycke av personuppgifter som behandlas i CNS:s studiestödsverksamhet är tillåtet bara i den utsträckning som medges i lag eller förordning och under förutsättning att bl.a. 8 § följs. Av 11 § följer att Försäkringskassan och arbetslöshetskassorna får ha direktåtkomst till personuppgifter som behandlas i CSN:s studiestödsverksamhet. Av 10 § framgår inte uttryckligen vem som har att följa sökbegränsningarna i 8 § i samband med att direktåtkomst tillåts, dvs. om föreskriften tar sikte på att reglera CSN:s med-

givande av direktåtkomst eller om den syftar till att begränsa Försäkringskassans och arbetslöshetskassornas användning av sökbegrepp vid deras sökningar via direktåtkomsten. Något klart svar ges inte heller i förarbetena (prop. 2008/09:96 s. 56 f.). En omständighet som inger betänkligheter i sammanhanget är att 10 § också hänvisar till bl.a. 6 § studiestödsdatalagen. I den paragrafen regleras i vilken utsträckning särskilda begränsningar gäller vid behandling av vissa särskilt känsliga personuppgifter. Begränsningarna innebär att dessa uppgifter bara får behandlas inom ramen för ett ärende i studiestödsverksamheten eller för att anmäla oegentligheter inom den verksamheten till ett offentligt organ som har att utreda eller beivra oegentligheterna. Eftersom Försäkringskassan och arbetslöshetskassorna inte ägnar sig åt sådan verksamhet, innebär det att direktåtkomsten över huvud taget inte kan komma till stånd om de myndigheterna också ska vara skyldiga att tillämpa 6 §. Det talar för att hänvisningen i 10 § studiestödsdatalagen till bl.a. 6 och 8 §§ samma lag inte tar sikte på behandling av personuppgifter hos de myndigheter som medges direktåtkomst utan på CNS:s egen verksamhet.

Det kan alltså konstateras att frågan om en mottagande myndighet vid direktåtkomst har att följa samma sökbegränsningar som gäller för den utlämnande myndigheten är beroende av hur gällande regelverk har utformats. Som framgått har vad som ska gälla reglerats på olika sätt.

11.3.2 Vad bör gälla i fortsättningen?

En rättslig utgångspunkt

Frågan om vilken betydelse sökförbud i en utlämnande myndighets registerförfattning har för bedömningen av vilka sammanställningar av personuppgifter som utgör allmänna handlingar hos den mottagande myndigheten aktualiseras endast vid uppgiftsutbyten mellan myndigheter som sker i form av direktåtkomst, inte vid andra utlämnanden i elektronisk form. Avgörande är att de båda myndigheterna har en gemensam tillgång till en viss informationssamling, dvs. den som omfattas av direktåtkomsten. När det gäller andra utlämnanden i elektronisk form uppstår inte samma problem, eftersom samma personuppgifter då inte behandlas gemensamt av ut-

lämnande och mottagande myndighet. Den behandling av personuppgifter som den mottagande myndigheten gör inom ramen för direktåtkomsten, dvs. genom att t.ex. söka fram uppgifter och eventuellt överföra uppgifter till sina egna informationssamlingar, utgör emellertid en del av den myndighetens verksamhet. Den behandling av personuppgifter som exempelvis Kronofogdemyndigheten utför när den använder sig av sin direktåtkomst hos Skatteverket sker alltså inom ramen för Kronofogdemyndighetens verksamhet och inte i den verksamhet som Skatteverket bedriver. De åtgärder som Skatteverket vidtar beträffande samma informationssamling, exempelvis genom att använda uppgifterna för egen del eller att uppdatera den information som finns, sker däremot i Skatteverkets verksamhet.

Vilket problem bör lösas?

Det kan förefalla orimligt att en enskild med stöd av 2 kap. 3 § andra stycket TF skulle kunna begära ut en sammanställning av personuppgifter hos en myndighet som den myndigheten har tillgång till genom direktåtkomst hos en annan myndighet, medan den enskilde inte hade kunnat få tillgång till sammanställningen hos den sistnämnda myndigheten på grund av att sökbegränsningar inte medger detta. Personuppgifterna har samlats in för den utlämnande myndighetens verksamhet och behandlingen har då, för att göra detta möjligt och väl avvägt med hänsyn till skyddet för personuppgifterna, omgärdats av vissa regler som begränsar hur uppgifterna får användas. Ett exempel på sådana skyddsregler kan vara sökbegränsningar. Om en sammanställning av uppgifter som är otillåten hos den insamlande myndigheten i stället kan begäras hos en annan myndighet tack vare att den medgetts direktåtkomst och inte behöver tillämpa sökbegränsningarna, kan det tyckas att uppgifterna på ett omotiverat sätt förlorar sitt skydd. Enligt Informationsutbytesutredningen är en sådan tolkning av rättsläget inte rimlig och kan inte ha varit lagstiftarens mening (SOU 2007:45 s. 199).

Vad som ska gälla i den aktuella frågan torde dock inte kunna besvaras med vad som ligger i sakens natur eller vad som kan anses rimligt. En bestämmelse som begränsar den grundlagsskyddade rätten att ta del av allmänna handlingar kan inte gärna tolkas annat än

enligt sin ordalydelse. Den fråga som i varje enskilt fall måste ställas är alltså om det i enlighet med vad som föreskrivs i 2 kap. 3 § tredje stycket TF finns en bestämmelse i lag eller förordning som innebär att den mottagande myndigheten saknar befogenhet att göra en sammanställning av uppgifter tillgänglig som myndigheten i och för sig kan nå via direktåtkomst hos en annan myndighet. Svaret torde ges i en eventuell registerförfattning på området. En mottagande myndighet saknar befogenhet att sammanställa uppgifter om det i en författning finns sökbegränsningar som förhindrar att uppgifter ur den aktuella informationssamlingen söks fram och de begränsningarna uttryckligen gäller även för den myndigheten.

Den omständigheten att en mottagande myndighet inte nödvändigtvis ska tillämpa samma sökbegränsningar som gäller för den utlämnande myndigheten innebär att myndigheten har befogenhet att även för sin egen verksamhet göra motsvarande sammanställning av de personuppgifter som den har tillgång till genom direktåtkomsten. Ur ett insynsperspektiv kan det anses rimligt att enskilda har möjlighet att ta del av samtliga sådana sammanställningar som en myndighet har befogenhet att göra. Det är syftet bakom den del av handlingsoffentligheten som tar sig uttryck i 2 kap. 3 § andra stycket TF och som har sin grund i den s.k. likställighetsprincipen, dvs. att enskilda i princip ska ha samma tillgång till en myndighets informationssamlingar som myndigheten själv har. Att en myndighets tillgång till information har sin grund i direktåtkomst kan knappast principiellt sett anses göra intresset av insyn i myndighetens verksamhet mindre.

Det går dock inte att komma ifrån att direktåtkomst ibland, p.g.a. att det tekniskt inte går att lösa på annat sätt eller av något annat skäl, medför att åtkomsten blir betydligt mer omfattande än vad motsvarande informationssamling hade blivit om myndigheten själv samlat in uppgifterna. Exempelvis innebär den åtkomst som socialnämnderna har till socialförsäkringsdatabasen att de har tillgång till personuppgifter från hela landet och inte endast rörande personer i den egna kommunen. Hade nämnden själv samlat in uppgifter hade de gjort det endast från sina kommuninvånare i den mån de var aktuella i ärenden hos nämnden. Nämndens åtkomst hade i så fall begränsats till personuppgifter i pågående och avslutade ärenden. De begränsningar som har införts för åtkomst till socialförsäkringsdatabasen i 114 kap. 22 och 23 §§ SFB tar emeller-

tid enbart sikte på att begränsa åtkomsten för den enskilde handläggaren hos nämnden som hanterar ett visst ärende. En sådan begränsning syftar alltså till att den enskilde handläggaren inte ska söka fram fler uppgifter än denne behöver för sitt ärende, dvs. en form av intern åtkomstregel. En sådan begränsning skulle inte utgöra ett sådant sökförbud som avses i 2 kap. 3 § tredje stycket TF även om uppgifterna hade samlats in av nämnden själv och därigenom fanns i dess informationssamlingar. För att åstadkomma ett sökförbud i tryckfrihetsförordningens mening krävs ett sökförbud som riktar sig till myndigheten som sådan, dvs. exempelvis att sökningar alltid måste avgränsas med uppgift om kommun.

Det förekommer alltså att en myndighet har medgetts direktåtkomst till en annan myndighets informationssamlingar utan att det övervägts om den myndighetens möjlighet att söka fram personuppgifter bör begränsas i samma utsträckning som gäller för den utlämnande myndigheten eller på annat sätt. I det sammanhanget räcker det alltså inte med att införa begränsningar som tar sikte på att den enskilde handläggaren inte ska söka fram fler uppgifter än denne behöver för stunden för att hantera ett visst ärende, utan det måste vara begränsningar som innebär ett sökförbud för myndigheten som sådan (se vidare vårt delbetänkande s. 149 f.).

Vår bedömning

Bedömning: Det är inte ändamålsenligt att förhindra eventuella risker för enskildas integritet i samband med direktåtkomst genom att föreskriva att samma sökbegränsningar alltid ska gälla för såväl den utlämnande myndigheten som den mottagande myndigheten. Det kan leda till att enskildas integritet inte skyddas i tillräcklig utsträckning, men också att en mottagande myndighets berättigade behov av att använda sig av de uppgifter som blir åtkomliga genom direktåtkomst inte kan tillgodoses.

Enskildas integritet bör i stället skyddas genom att en direktåtkomst inte medges förrän noggranna överväganden har gjorts beträffande den mottagande myndighetens användning av direktåtkomsten, bl.a. beträffande vilka sökbegränsningar som den ska iaktta.

Direktåtkomst medges för att åstadkomma ett så effektivt uppgiftsutbyte som möjligt. Skälet till att direktåtkomst medges är alltså att spara resurser, både hos den utlämnande och mottagande myndigheten. Den mottagande myndigheten medges direktåtkomst för att själv slippa samla in de aktuella uppgifterna eller för att undvika ett mer tidskrävande sätt att få tillgång till uppgifterna, t.ex. att de lämnas ut efter en manuell hantering av den utlämnande myndigheten. En förutsättning för att direktåtkomsten ska uppfylla sitt syfte med att vara effektiv för den mottagande myndigheten torde vara att den myndigheten får använda de uppgifter som den får tillgång till på ett sätt som är ändamålsenligt i den myndighetens verksamhet. Den omständigheten bör enligt vår uppfattning utgöra en självklar utgångspunkt i frågan om den mottagande myndigheten ska vara bunden av samma sökbegränsningar som gäller för den utlämnande myndighetens behandling av personuppgifter.

Det förekommer att en myndighet medges direktåtkomst till en annan myndighets informationssamlingar trots att deras verksamheter skiljer sig åt på ett avgörande sätt. Ett exempel på det är brottsenheterna inom Skatteverket som medgetts direktåtkomst till beskattningsdatabasen, trots att uppgifterna där har samlats in för beskattningsverksamheten och många gånger genom att skattskyldiga och andra själva har lämnat uppgifter till Skatteverket på grund av att de är skyldiga att göra det. Lagstiftaren har emellertid bedömt att direktåtkomsten kan medges och har utfärdat regler som avses skydda personuppgifterna så att direktåtkomsten inte medför otillbörliga intrång i enskildas integritet. Det har åstadkommits både genom att direktåtkomsten som sådan har begränsats till vissa uppgifter och att det införts begränsningar i skattebrottsenheternas möjlighet att söka fram uppgifter genom direktåtkomsten.

För att åstadkomma en rimlig avvägning mellan effektivitet och hänsyn till enskildas integritet då direktåtkomst medges till personuppgifter som i den enskildes perspektiv kan vara känsliga för spridning, dvs. företrädesvis sekretessreglerade personuppgifter, behöver således ett helt ”paket” av föreskrifter komma på plats. Det gäller i första hand att direktåtkomst inte medges till fler uppgifter än vad den mottagande myndigheten behöver och vad som i övrigt kan anses rimligt. Även nödvändiga sekretessbestämmelser behöver in-

föras och föreskrifter som reglerar den mottagande myndighetens användning av direktåtkomsten, exempelvis i form av sökbegränsningar. Om inte alla dessa delar har övervägts och nödvändiga författningsändringar har gjorts, finns det risk för att direktåtkomsten får allvarliga konsekvenser för den enskildes skydd för sina personuppgifter.

I registerförfattningar har frågan om vad som ska gälla i fråga om mottagande myndighets sökbegränsningar rörande de personuppgifter som den får tillgång till genom direktåtkomst reglerats på olika sätt och inte alltid – förfaller det – i alla delar helt genomtänkt. Det kan inte anses tillfredsställande att det inte är tydligt vilken eller vilka myndigheter som har att tillämpa en bestämmelse om sökbegränsningar, eftersom sådana begränsningar utgör ett viktigt verktyg för att motverka att myndigheter söker fram personuppgifter ur informationssamlingar som de i och för sig har tillgång till, men där uppgifterna varken är motiverade eller proportionerliga i förhållande till det uppdrag som myndigheten har att utföra. Det är inte heller tillfredsställande att det kan finnas tvekan om i vilken mån det faktiskt föreligger hinder för myndigheten att på begäran av enskilda enligt 2 kap. 3 § TF tillhandahålla sammanställningar av personuppgifter.

Det kan förefalla som en enkel lösning att exempelvis i den nya lagen föreskriva att sökbegränsningar som gäller för den utlämnande myndigheten alltid ska gälla för en annan myndighet som medges direktåtkomst till myndighetens informationssamlingar. Frågan är dock om det vore det mest ändamålsenliga sättet att förhindra eventuella risker för enskildas integritet i samband med direktåtkomst. Det skulle kunna vara så att de sökbegränsningarna inte kan anses tillräckliga för att skydda enskildas integritet i den mottagande myndighetens verksamhet. Som exempel kan nämnas att Skatteverkets brottsenheter har mer begränsande sökmöjligheter vid användningen av sin direktåtkomst till beskattningsdatabasen än vad Skatteverket har i sin beskattningsverksamhet. Man kan också tänka sig det motsatta fallet, dvs. att den mottagande myndighetens berättigade behov av att använda sig av de personuppgifter som blir åtkomliga genom direktåtkomsten innebär att bestämmelser om sökförbud som ska tillämpas av den myndigheten behöver utformas på ett mindre inskränkande sätt än för den utlämnande myndigheten. Så skulle exempelvis kunna vara fallet om en

myndighet ska utföra ett uppföljnings- eller forskningsuppdrag och därför kan ha behov av göra andra sammanställningar i den informationssamling som blir åtkomlig genom direktåtkomsten än sådana som kan anses motiverade för den utlämnande myndighetens behov.

Enligt vår bedömning bör skyddet för enskildas integritet snarare åstadkommas genom att det i samband med att man avser att medge direktåtkomst till uppgifter gör noggranna överväganden när det gäller vad som ska gälla i fråga om den mottagande myndighetens användning av direktåtkomsten. Bland annat bör man ta ställning till om den mottagande myndigheten har att iaktta sökbegränsningar som utgör ett tillräckligt skydd även för de personuppgifter som kan sökas fram via direktåtkomsten. Om inte, bör lagstiftaren se till att den mottagande myndigheten ska iaktta ytterligare begränsningar genom författningsreglering av sökbegränsningar. Utformningen av det regelverk som gäller för behandling av personuppgifter i aktuell verksamhet eller för ett visst register får därvid styra vad som ska anses vara den lämpligaste platsen för sådan reglering.

Vi har i avsnitt 9.4 behandlat frågan om den nya lagen bör innehålla sökbegränsningar som gäller generellt för myndigheter.

12 Överföring till tredjeland

12.1 Allmänna dataskyddsrättsliga regler

Dataskyddsdirektivet

Syftet med dataskyddsdirektivet har varit att skapa en gemensam, hög nivå på integritetsskyddet vid behandling av personuppgifter för att därigenom möjliggöra ett fritt flöde av personuppgifter medlemsstaterna emellan. Direktivet har också införts i övriga stater som är anslutna till Europeiska ekonomiska samarbetsområdet (EES). Ett motsvarande fritt flöde av personuppgifter till tredjeland är däremot inte möjligt. Det har emellertid genom direktivet lagts fast en gemensam nivå på skyddet för personuppgifterna visavi tredjeland för att möjliggöra överföringar till stater utanför EU/EES.

Kapitel IV i dataskyddsdirektivet med artiklarna 25 och 26 innehåller bestämmelser om överföring av personuppgifter till tredjeland.

Enligt artikel 25.1 ska medlemsstaterna föreskriva att överföringen av personuppgifter som är under behandling eller som är avsedda att behandlas efter överföring till tredjeland endast får ske om det tredjelandet – utan att detta påverkar tillämpningen av de nationella bestämmelser som har antagits till följd av de andra bestämmelserna i direktivet – säkerställer en adekvat skyddsnivå.

Bedömningen av om skyddsnivån i ett tredjeland är adekvat ska enligt artikel 25.2 ske på grundval av alla de förhållanden som har samband med en överföring eller en grupp av överföringar av uppgifter. Särskilt ska beaktas uppgiftens art, den eller de avsedda behandlingarnas ändamål och varaktighet, ursprungslandet och det slutliga bestämmelselandet, de allmänna respektive särskilda rättsregler som gäller i ifrågavarande tredjeland liksom de regler för yrkesverksamhet och säkerhet som gäller där.

Kommissionen kan besluta att ett tredjeland har en adekvat skyddsnivå. Medlemsstaterna ska se till att kommissionens beslut följs (artikel 25.6). Kommissionen har meddelat ett antal sådana beslut som omfattar vissa länder eller specificerade mottagare i vissa länder (jfr bilaga 1 till personuppgiftsförordningen). Som exempel kan nämnas kommissionens beslut att en adekvat skyddsnivå uppnås i USA genom de principer om integritetsskydd – Safe Harbour Privacy Principles – som gäller på frivillig väg genom att organisationer ansluter sig till en uppsättning dataskyddsregler som det amerikanska handelsdepartementet har utformat.

Kommissionen kan också i beslut slå fast att tredjeland *inte* erbjuder en adekvat skyddsnivå (artikel 25.4).

I artikel 26 föreskrivs vissa undantag som innebär att överföring till tredjeland kan få ske trots att det tredjelandet inte har en adekvat skyddsnivå för personuppgifterna. Motsatsvis gäller således ett förbud mot överföring, dvs. om skyddsnivån inte är adekvat och något undantag inte gäller.

Undantag från förbudet gäller enligt artikel 26.1 om

a) den registrerade otvetydigt har samtyckt till den planerade överföringen,

b) överföringen är nödvändig för att fullgöra ett avtal mellan den registrerade och den registeransvarige eller för att på den registrerades begäran genomföra åtgärder som vidtas innan avtalet ingås,

c) överföringen är nödvändig för att ingå eller fullgöra ett avtal mellan den registeransvarige och tredje man i den registrerades intresse,

d) överföringen är nödvändig eller bindande enligt författning av skäl som rör viktiga allmänna intressen eller för att fastslå, göra gällande eller försvara rättsliga anspråk,

e) överföringen är nödvändig för att skydda intressen som är av avgörande betydelse för den registrerade, eller

f) överföringen görs från ett offentligt register som enligt lagar eller andra författningar är avsett att ge allmänheten information och som är tillgängligt antingen för allmänheten eller för var och en som kan styrka ett berättigat intresse, i den utsträckning som de

i lagstiftningen angivna villkoren för tillgänglighet uppfylls i det enskilda fallet.

I punkt 58 i ingressen till direktivet anges internationellt utbyte av uppgifter mellan skattemyndigheter eller tullmyndigheter eller mellan socialförsäkringsmyndigheter som exempel på viktiga allmänna intressen.

Därutöver får en medlemsstat enligt artikel 26.2 tillåta överföring av personuppgifter till ett tredjeland som inte säkerställer en skyddsnivå som är adekvat, om den registeransvarige ställer tillräckliga garantier för att privatliv och enskilda personers grundläggande fri- och rättigheter skyddas samt för utövningen av motsvarande rättigheter. Sådana garantier kan framgå av lämpliga avtalsklausuler. Kommissionen kan med bindande verkan för medlemsstaterna besluta att vissa standardavtalsklausuler erbjuder tillräckliga garantier (artikel 26.4). Så har också skett, bl.a. i fråga om överföring av personuppgifter till personuppgiftsbiträden i tredjeland (jfr bilaga 2 till personuppgiftsförordningen).

Personuppgiftslagen

Dataskyddsdirektivets bestämmelser om överföring till tredjeland har genomförts i Sverige genom 33–35 §§ PuL samt genom ytterligare bestämmelser i personuppgiftsförordningen. I förarbetena till personuppgiftslagen framhölls att direktivets bestämmelser om överföring till tredjeland är detaljerade och komplicerade. En mer komplicerad reglering än vad som var nödvändigt borde därför inte införas i lagstiftningen (prop. 1997/98:44 s. 95 f.). Det bedömdes därvid som nödvändigt att i personuppgiftslagen införa ett förbud mot överföring till tredjeland liksom de konkreta undantag från förbudet som räknas upp i direktivet. Vidare har regeringen eller den myndighet regeringen bestämmer, dvs. Datainspektionen, bemyndigats att meddela föreskrifter om ytterligare undantag från förbudet mot överföring.

Den ursprungliga regleringen i personuppgiftslagen ändrades den 1 januari 2000 genom att förbudet modifierades till att bara gälla fall då det saknas en adekvat skyddsnivå i det tredjelandet (prop. 1999/2000:11). Ändringen syftade till att skapa ökat utrymme för

användning av internet och andra elektroniska kommunikationsnätverk såsom e-post.

I 33 § första stycket PuL anges huvudregeln. Den föreskriver ett förbud mot överföring av personuppgifter som är under behandling till tredjeland som inte har en adekvat nivå för skyddet av personuppgifter. Förbudet avser även överföring av personuppgifter för behandling. Bestämmelsen överensstämmer i sak med artikel 25.1 i direktivet dock att den föreskriver ett förbud i stället för att, såsom i direktivet, ange under vilka förutsättningar överföring kan tillåtas.

I 33 § andra stycket PuL anges hur frågan om adekvat skyddsnivå ska bedömas. Detta ska ske med hänsyn till samtliga omständigheter som har samband med överföringen. Särskild vikt ska läggas vid uppgifternas art, ändamålet med behandlingen, hur länge behandlingen ska pågå, ursprungslandet, det slutliga bestämmelselandet och de regler som finns för behandlingen i det tredjelandet.

Huruvida det finns en adekvat skyddsnivå ska alltså bedömas beroende på omständigheterna i det enskilda fallet. Det har ansetts att skyddsnivån kan vara adekvat även om dataskydd helt saknas i det tredjelandet, nämligen om det beroende på omständigheterna inte finns något behov av skydd. Ett tredjeland kan vidare ha adekvat skydd på något område men inte på andra (prop. 1999/2000:11 s. 15 f.). Klart är att, som bestämmelsen i 33 § andra stycket formulerats, det ankommer på den personuppgiftsansvarige att i det enskilda fallet göra en bedömning av skyddsnivån med ledning av de faktorer som anges i bestämmelsen. Den personuppgiftsansvarige anses ha bevisbördan för att skyddsnivån i det tredjelandet är adekvat (a. prop. s. 20).

Det bör dock framhållas att överföring av personuppgifter till ett tredjeland inte per automatik är en tillåten personuppgiftsbehandling bara därför att tredjelandet har en adekvat skyddsnivå. Behandlingen som sådan måste vara tillåten också enligt personuppgiftslagens övriga bestämmelser, exempelvis vara förenlig med de grundläggande kraven i 9 §, vara tillåten med stöd av någon av de rättsliga grunderna i 10 § och omfattas av tillräckliga säkerhetsåtgärder enligt 31 §.

Enligt 34 § första stycket PuL är överföring trots avsaknad av adekvat skyddsnivå tillåten om den enskilde har lämnat sitt samtycke till överföringen eller om överföringen är nödvändig för att

a) ett avtal mellan den registrerade och den personuppgiftsansvarige ska kunna fullgöras eller åtgärder som den registrerade begärt ska kunna vidtas innan ett avtal träffas,

b) ett sådant avtal mellan den personuppgiftsansvarige och tredje man som är i den registrerades intresse ska kunna ingås eller fullgöras,

c) rättsliga anspråk ska kunna fastställas, göras gällande eller försvaras, eller

d) vitala intressen för den registrerade ska kunna skyddas.

I dessa fall krävs således inte att det finns någon adekvat skyddsnivå för personuppgifterna i mottagarlandet. Bestämmelserna i 34 § första stycket är avsedda att ha samma innebörd som artikel 26.1 i direktivet. Det kan dock noteras att det inte finns någon uttrycklig motsvarighet till direktivets undantag i 26.1 punkt f vilket torde sammanhänga med att den typ av offentliga register som där avses regleras i särskilda registerförfattningar som har företräde framför personuppgiftslagen enligt 2 § PuL. Vidare har artikel 26.1 punkt d om överföring av skäl som rör viktiga allmänna intressen genomförts på så sätt att regeringen, eller den myndighet regeringen bestämmer, getts befogenhet att meddela undantag om det behövs med hänsyn till ett viktigt allmänt intresse (35 § andra stycket PuL).

I 34 § andra stycket anges att det är tillåtet att överföra personuppgifter för användning enbart i en stat som har anslutit sig till Europarådets dataskyddskonvention. Bestämmelsen har ingen motsvarighet i direktivet. Bakgrunden till bestämmelsen är att Sverige till följd av artikel 12 i konventionen inte av integritetsskyddsskäl får hindra att personuppgifter förs över till en annan konventionsstat för att användas där. I förarbetena anförs att konventionsstater får anses ha sådan adekvat skyddsnivå som krävs enligt direktivet (prop. 1997/98:44. s. 96).

Enligt 35 § första stycket PuL får regeringen meddela ytterligare föreskrifter om undantag från förbudet i 33 §. Det gäller dels föreskrifter om undantag för överföring av personuppgifter till vissa stater, dels föreskrifter om att överföring av personuppgifter till tredjeland är tillåten om överföringen regleras av ett avtal som ger tillräckliga garantier till skydd för de registrerades rättigheter. Regeringen har i 13 § PuF meddelat bestämmelser med stöd av 35 § PuL. Av 13 § första stycket 1 PuF följer att överföring till tredjeland får

ske om och i den utsträckning kommissionen i enlighet med artikel 25.6 i direktivet har beslutat att ett land eller specificerade mottagare i ett land har en adekvat skyddsnivå. Kommissionens beslut anges i bilaga 1 till personuppgiftsförordningen. Enligt 13 § första stycket 2 får överföring ske med tillämpning av avtal med sådana standardavtalsklausuler som kommissionen har beslutat om enligt artikel 26.4 i direktivet. Dessa beslut anges i bilaga 2 till personuppgiftsförordningen.

I 35 § andra stycket PuL anges vidare att regeringen får meddela föreskrifter om undantag från förbudet i 33 § om det behövs med hänsyn till ett viktigt allmänt intresse eller om det finns tillräckliga garantier till skydd för de registrerades rättigheter. Regeringen har genom 14 § PuF vidaredelegerat föreskriftsrätt till Datainspektionen som får meddela föreskrifter om undantag om det finns tillräckliga garantier till skydd för de registrerades intresse. Däremot har Datainspektionen inte bemyndigats att meddela föreskrifter om undantag som kan behövas med hänsyn till ett viktigt allmänt intresse.

I 12 § PuF finns vidare bestämmelser som ger kommuner, landsting och kommunalförbund rätt att under vissa förutsättningar överföra personuppgifter till tredjeland på grund av ett viktigt allmänt intresse. Av paragrafen följer att diarium enligt 5 kap. 2 § OSL samt kallelse till, kungörelse om och justerat protokoll från sammanträde i fullmäktige eller nämnd får med vissa undantag överföras till tredjeland. Syftet med bestämmelsen, som trädde i kraft den 1 januari 2001, var att underlätta för kommuner att publicera personuppgifter på internet. Det kan diskuteras i vilken mån regleringen numera har någon egentlig praktisk betydelse (jfr EU-domstolens dom den 6 november 2003 i mål C-101/01, se nedan).

Enligt 35 § tredje stycket PuL får regeringen i enskilda fall besluta om undantag under de förutsättningar som nämns i paragrafens andra stycke. Regeringen kan också överlåta åt tillsynsmyndigheten att fatta sådana beslut. Datainspektionen har genom 14 § PuF getts möjlighet att fatta sådana beslut i enskilda fall förutsatt att det finns tillräckliga garantier till skydd för de registrerades rättigheter.

Förbudet och undantagsbestämmelserna rörande överföring av personuppgifter till tredjeland hör till de regler i personuppgiftslagen som räknas upp i den s.k. missbruksregeln i 5 a §. Det innebär att 33 och 34 §§ inte behöver tillämpas på behandling av personuppgifter som inte ingår i eller är avsedda att ingå i en samling av

personuppgifter som har strukturerats för att påtagligt underlätta sökning efter eller sammanställning av personuppgifter, dvs. behandling i ostrukturerat material, och som inte heller är kränkande.

I motiven till 5 a § PuL anfördes när det gäller överföring till tredjeland att man i princip skulle kunna hävda att en överföring av personuppgifter i ostrukturerat material, som inte innefattar ett missbruk av personuppgifterna, innebär en överföring till ett land med adekvat skyddsnivå, eftersom, med hänsyn till omständigheterna vid överföringen, någon särskild skyddsnivå inte krävs i det mottagande landet. En sådan överföring skulle därmed vara tillåten redan enligt gällande rätt (dvs. 33 §). Personuppgiftslagsutredningen, på vars förslag missbruksregeln bygger, hade emellertid ansett att stöd för att göra undantag från överföringsförbudet för ostrukturerat material i första hand borde hämtas i artikel 26.1 d. Enligt den artikeln kan överföring till tredjeland utan adekvat skyddsnivå tillåtas om det är nödvändigt av t.ex. skäl som rör viktiga allmänna intressen. Hantering av personuppgifter i ostrukturerat material, t.ex. i form av löpande text och ljud- och bildupptagningar, kan ha betydelse för bl.a. utnyttjandet av yttrande- och informationsfriheten som kan anses vara en fri- och rättighet. Att fri- och rättigheter kan utövas i samhället är naturligtvis ett allmänt intresse och dessutom ett viktigt sådant. Regeringen anförde att oavsett vilket synsätt man anlägger på frågan blir slutsatsen densamma; en överföring till tredjeland av personuppgifter i ostrukturerat material, som inte innefattar ett missbruk av personuppgifterna, står inte strid med direktivet (prop. 2005/06:173 s. 35).

Förslaget till uppgiftsskyddsförordning

Kommissionen

I likhet med dataskyddsdirektivet reglerar förslaget till förordning under vilka förutsättningar personuppgifter får överföras till tredjeland. Bestämmelserna finns samlade i artiklarna 40–45. Den föreslagna regleringen innebär en vidareutveckling av motsvarande reglering i dataskyddsdirektivet. En nyhet är att bestämmelserna även gäller överföring till en internationell organisation utanför EU (artikel 40). Regleringen är förhållandevis detaljerad och i det följande

redovisas bara sådant som bedömts vara av särskilt intresse för vårt arbete.

Liksom i dataskyddsdirektivet är det enligt artikel 41 i förordningen ett grundläggande krav för sådan överföring att det mottagande tredjelandet säkerställer en adekvat skyddsnivå för uppgifterna. Det är kommissionen som ska besluta om ett tredjeland uppfyller detta krav eller inte. Sådana beslut får direkt verkan i medlemsstaterna. De kriterier utifrån vilka kommissionen ska göra denna bedömning har utvidgats i förhållande till direktivet till att omfatta bl.a. rättsstatsprincipen, tillgången till rättslig prövning och oberoende tillsyn i mottagarlandet.

Har kommissionen inte fattat något beslut i frågan om adekvat skyddsnivå, finns det möjlighet att överföra uppgifter till tredjeland om vissa juridiskt bindande skyddsåtgärder vidtas, som t.ex. användandet av vissa godkända standardbestämmelser om uppgiftsskydd. Detta följer av artikel 42 som alltså bygger på artikel 26.4 i direktivet. En nyhet är emellertid att standardiserade uppgiftsskyddsbestämmelser kan antas inte bara av kommissionen utan även av en nationell tillsynsmyndighet i en medlemsstat och av kommissionen sedan förklaras vara allmänt giltiga. En registeransvarig eller registerförare kan vidare överföra personuppgifter efter godkännande från en tillsynsmyndighet av avtalsklausuler mellan den registeransvarige eller registerföraren och mottagaren av uppgifterna.

Artikel 44 innehåller bestämmelser om överföring då det varken finns adekvat skyddsnivå enligt artikel 41 eller lämpliga skyddsåtgärder enligt artikel 42. Bestämmelserna motsvarar i huvudsak artikel 26.1 i direktivet, dock med några justeringar och tillägg.

Det ska även fortsättningsvis vara tillåtet med överföring om den registrerade samtyckt till överföringen. Dock krävs enligt artikel 44.1 a att den registrerade först har blivit informerad om de risker en överföring kan medföra när det inte föreligger något beslut om adekvat skyddsnivå eller lämpliga skyddsåtgärder. Vidare får enligt artikel 44.1 d överföring ske om den bedöms gynna viktiga samhälleliga intressen. Allmänhetens intresse får dock bara åberopas om intresset har stöd i unionslagstiftning eller i den medlemsstats lagstiftning som är tillämplig på den registeransvarige (artikel 44.5). Dessutom föreskrivs att kommissionen får anta delegerade akter i syfte att precisera villkoren för vad som bedöms ”gynna viktiga samhälleliga intressen” (artikel 44.7).

Enligt artikel 44.4 gäller bestämmelserna om undantag för det som i dag motsvarar artikel 26.1 b och c i direktivet (34 § första stycket a och b PuL) inte åtgärder som vidtas av offentliga myndigheter som en del av deras offentliga befogenheter.

Liksom i dataskyddsdirektivet föreskrivs undantag i fråga om överföring från ett register som enligt unionens eller medlemsstatens lagstiftning är avsett att ge allmänheten information och som är tillgängligt antingen för allmänheten eller för var och en som kan styrka ett berättigat intresse, i den utsträckning som de i unionslagstiftningen eller medlemsstatens lagstiftning angivna villkoren för tillgänglighet uppfylls i det enskilda fallet, artikel 44.1. g. Enligt artikel 44.2 får inte överföringen omfatta alla personuppgifter eller hela kategorier av personuppgifter som finns i registret. Om registret är avsett att vara tillgängligt för personer med ett berättigat intresse ska överföringen göras endast på begäran av dessa personer eller om de själva är mottagarna.

Ett nytt undantag föreslås i artikel 44.1 h enligt vilket överföring under vissa begränsade omständigheter får ske för att tillgodose den registeransvariges berättigade intressen. Det undantaget ska dock inte vara tillämpligt på åtgärder som vidtas av offentliga myndigheter som en del av deras offentliga befogenheter.

Europaparlamentet

Europaparlamentet har vid sin behandling av förordningen lämnat ett mindre antal ändringsförslag i regleringen av överföring till tredjeland. Av intresse här är närmast att parlamentet strukit förslaget i 44.7 om att kommissionen ska kunna anta delegerade akter om villkoren för vad som kan bedömas gynna samhälleliga intressen. I stället föreslås att Europeiska dataskyddsstyrelsen ska anförtros uppgiften att utfärda riktlinjer, rekommendationer och ”best practices”. Vidare föreslår parlamentet att förslaget om ett nytt undantag från förbudet mot överföring till tredjeland efter en intressebedömning utgår, se ovan angående artikel 44.1 h.

Några kommentarer

Många av de föreslagna bestämmelserna om överföring av personuppgifter till tredjeland företer alltså stora likheter med dataskyddsdirektivet. Men det finns också betydande skillnader. En väsentlig sådan är att kommissionen föreslås få en exklusiv behörighet att göra bedömningar av vad som utgör adekvat skyddsnivå i tredjeland. Den personuppgiftsansvariges möjlighet att göra en egen bedömning utifrån regleringen i 33 § PuL och de faktorer som där anges ska beaktas tycks helt upphöra. Likaså medför förslaget till förordning att det inte kommer att finnas något utrymme att utforma nationell lagstiftning om överföring av personuppgifter till tredjeland utifrån bedömningar av vilken adekvat skyddsnivå som krävs för olika fall.

När det gäller undantaget för överföring för det som i direktivet benämns viktiga allmänna intressen men som i förordningen uttrycks med att överföringen bedöms gynna viktiga samhälleliga intressen går det knappast att dra några säkra slutsatser om i vilken mån den nya ordalydelsen innebär någon förändring i sak. Någon tydlig avsikt till ändring av tillämpningsområdet går i vart fall inte att utläsa av förslaget.

Den föreslagna bestämmelsen i artikel 44.5 om att allmänhetens intresse enligt 44.1 d bara får åberopas om det har stöd i unionslagstiftningen eller i den medlemsstat lagstiftning som är tillämplig på den registeransvarige torde, liksom hittills, möjliggöra nationell lagstiftning om direkta undantag från överföringsförbudet med hänsyn till det angivna intresset.

12.2 Vad avses med begreppet överföring?

Som har framgått omfattar överföringsförbudet både personuppgifter som är under sådan behandling som omfattas av personuppgiftslagens tillämpningsområde, dvs. behandling som är helt eller delvis automatiserad eller sker i manuella register, och personuppgifter som är avsedda att behandlas i mottagarlandet. I den engelska versionen av direktivet uttrycks detta med att det ska handla om ”transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer”.

Det saknas vägledande avgöranden i rättspraxis om vad som rent faktiskt är att se som överföring. I litteraturen har det förts viss diskussion om vad som ska förstås med begreppet. I vilken mån det ska ses som en överföring att befinna sig i ett tredjeland och där ha elektronisk tillgång till personuppgifter som ”finns” i hemlandet är t.ex. oklart. Vad som ska anses gälla om en företrädare för en personuppgiftsansvarig rent fysiskt tar med sig personuppgifter, t.ex. i en bärbar dator, på en tillfällig resa till tredjeland är också omdiskuterat.

Enligt vår uppfattning är det emellertid en rimlig tolkning att det knappast kan vara fråga om en överföring av personuppgifter till tredjeland bara genom att en person befinner sig utanför EU/EES med personuppgifter i sin besittning. Det krävs rimligen i vart fall en avsikt att personuppgifterna ska nå en mottagare i tredjeland för att det ska vara fråga om en överföring i lagens mening. Det är en annan sak, menar vi, att ”medförande” av personuppgifter till tredjeland kräver särskilda överväganden när det gäller upprätthållandet av tillräcklig säkerhet till skydd för personuppgifterna.

Hur rekvisitet ”under behandling” ska förstås är också oklart. Definitionen i 3 § PuL av begreppet behandling av personuppgifter är vidsträckt. I princip alla slags åtgärder omfattas av begreppet. Det synsättet kunde därför anläggas att rekvisitet ”under behandling” rimligen bör kopplas till det slags behandling som omfattas av personuppgiftslagens tillämpningsområde såsom detta anges i 5 § PuL. Det skulle då alltså – bortsett från vissa manuella register – bara vara personuppgifter som behandlas helt eller delvis automatiserat, dvs. elektroniskt, som alls träffas av regleringen. Huruvida man sedan bör betrakta själva överföringen som en separat behandling, skild från den behandling som annars äger rum hos den personuppgiftsansvarige, är en annan sak.

Om utskrifter av personuppgifter skickas i pappersform per post så kunde det i så fall hävdas att det inte är fråga om en överföring i nu aktuell mening, förutsatt att överföringen inte syftar till automatiserad behandling i mottagarlandet. Vid en sådan överföring är uppgifterna nämligen inte ”under behandling” på sätt som anges i 33 § första stycket första meningen PuL (jfr artikel 25.1 i direktivet). Om syftet däremot är att personuppgifterna i pappershandlingarna ska föras över till ett manuellt register, till dator eller på annat sätt behandlas elektronisk i mottagarlandet skulle det

däremot vara fråga om överföring till tredjeland i personuppgiftslagens och direktivets mening så länge uppgifterna överförs i detta syfte, dvs. ”för behandling”. Ett exempel kan vara enkätundersökningar med personuppgifter där svarsblanketter på papper skickas till tredjeland för statistisk bearbetning och analys i elektronisk form. Även beträffande 33 § första stycket andra meningen skulle man alltså måhända kunna anlägga det synsättet att med behandling avses sådan behandling som omfattas av 5 § – helt eller delvis automatiserad sådan eller i manuella register – snarare än vad som faller in under definitionen av behandling i 3 §.

Men det kan alltså också förhålla sig på det viset att med ”behandling” ska förstås detsamma som anges i 3 § PuL. Det skulle exempelvis innebära att det innebär en överföring av personuppgifter till tredjeland att sända över pappersutskrifter av elektroniskt lagrade personuppgifter.

Vad som omfattas av begreppet överföring av personuppgifter är alltså oklart. Såvitt är aktuellt nu kan man emellertid konstatera att en överföring i vart fall torde äga rum när en myndighet i något syfte skickar, vidarebefordrar eller förmedlar information i elektronisk form till en mottagare som befinner sig i tredjeland, alltså utanför EU/EES.

Det bör vidare observeras att bestämmelserna om överföring till tredjeland gäller för alla slags personuppgifter. Samma regler gäller i princip för indirekta personuppgifter som överförs kodade med kodnyckeln bevarad i Sverige som för i personuppgiftslagens mening känsliga personuppgifter. En annan sak är att uppgifternas art givetvis är en omständighet som ska beaktas när det ska bedömas vilken skyddsnivå som kan bedömas vara påkallad, dvs. adekvat.

Det krävs inte att överföringen till tredjeland måste innebära att personuppgifter lämnas ut till tredje man (se definitionen av tredje man i 3 § PuL). Det är således fråga om en överföring till tredjeland även om personuppgifterna bara lämnas till ett personuppgiftsbiträde i tredjeland för att faktiskt behandlas där, t.ex. om en myndighet använder sig av en tillhandahållare av en it-tjänst. Detta framgår implicit av de standardavtalsvillkor som kommissionen beslutat om rörande överföring av personuppgifter till registerförare i tredjeland.

När det gäller publicering på internet antogs tidigare av den svenske lagstiftaren att all öppen publicering på en webbplats som är allmänt tillgänglig på internet innebär att personuppgifterna blir

tillgängliga i hela världen och därmed kan anses överförda till alla länder i direktivets mening (jfr bl.a. prop. 1999/2000:11 s. 11 f.). EU-domstolen har emellertid i det s.k. konfirmandlärarmålet (dom den 6 november 2003 i mål C-101/01, Lindgren) slagit fast att det inte är fråga om någon överföring av uppgifter till tredjeland i direktivets mening när en person, som befinner sig i en medlemsstat, lägger ut personuppgifter på en webbplats på internet som är lagrad hos en fysisk eller juridisk person som har den webbplats där man kan komma åt sidan och som är etablerad i samma medlemsstat eller i en annan medlemsstat, varvid uppgifterna blir åtkomliga för alla som kopplar upp sig på internet, inklusive personer i tredjeland.

Viss diskussion har förekommit beträffande hur långt EU-domstolens uttalande sträcker sig (se t.ex. SOU 2004:6 s. 233). I NJA 2005 s. 361 ansågs en rektor på en enskilt bedriven skola inte ha överfört personuppgifter till tredjeland genom att publicera uppgifterna på skolans webbplats. Svea hovrätt har gjort samma bedömning i likartade fall (dom 2004-08-31 i mål nr B 4151-04 respektive 2004-11-16 i mål nr B 7837-03).

E-offentlighetskommittén fann att EU-domstolens avgörande klarlagt att tillgängliggörande av information genom utläggning på internet i de flesta fall inte innebär överföring till tredjeland i dataskyddsdirektivets mening. Det anses i princip inte som en tredjelandsöverföring om uppgifterna publiceras på en webbplats på internet och webbplatsen lagras hos en internetleverantör som är etablerad inom EU. Enligt kommittén bör det alltså inte ses som överföring i strid med 33 § PuL om en myndighet lägger ut information från ett s.k. allmänt register på sin hemsida så länge den aktuella servern finns inom EU-området (SOU 2010:4 s. 338).

Utlänningar är i princip likställda med svenska medborgare när det gäller rätten att begära ut allmänna handlingar enligt 2 kap. TF. Att lämna ut personuppgifter i allmänna handlingar är en form av behandling av personuppgifter. Utlämnanden av allmänna handlingar till mottagare i tredjeland torde också – beroende på omständigheterna – kunna utgöra överföring i personuppgiftslagens mening, i vart fall om utlämnandet sker i elektronisk form. En annan sak är att personuppgiftslagens regler inte tillämpas i den mån det skulle inskränka en myndighets skyldighet enligt 2 kap. TF att lämna ut uppgifter. Vi återkommer till detta nedan.

12.3 Reglering i registerförfattningar

Det hör till sällsyntheterna att registerförfattningar för myndigheters behandling av personuppgifter innehåller reglering av möjligheterna att överföra personuppgifter till tredjeland som avviker från vad som följer av 33–35 §§ PuL eller föreskrifter som meddelats med stöd av personuppgiftslagen. I det stora flertalet fall gäller alltså personuppgiftslagens bestämmelser. Detta framgår genom att det antingen hänvisas till att 33–35 §§ PuL är tillämpliga eller så gäller dessa bestämmelser outtalat därför att registerförfattningen i fråga saknar bestämmelser om överföring till tredjeland och författningen är så konstruerad att personuppgiftslagen ska tillämpas i den mån ett förhållande inte regleras i registerförfattningen.

I den kategori registerförfattningar som vi kallar informationshanteringsförfattningar är det enbart på socialförsäkringsområdet som detta mönster bryts. Enligt 114 kap. 29 § SFB får, utan hinder av 33 § PuL, överföring ske av personuppgifter till tredjeland på grund av åtaganden i avtal om social trygghet som Sverige ingått med andra stater. Detta torde vara en bestämmelse om undantag som ligger väl i linje med vad som uttalats i punkt 58 i ingressen till direktivet om internationellt utbyte av uppgifter mellan socialförsäkringsmyndigheter såsom exempel på viktiga allmänna intressen.

Bland mer renodlade registerförfattningar där det förekommer särbestämmelser om överföring kan nämnas förordningen (2001:720) om behandling av personuppgifter i verksamhet enligt utlännings- och medborgarskapslagstiftningen av vilken följer att Migrationsverket får till tredjeland föra över personuppgifter som finns i verkets rättsfallsregister (8 §). Det kan observeras att det registret inte får innehålla uppgifter som direkt pekar ut en enskild registrerad. Ett annat exempel är 23 § rättsinformationsförordningen (1999:175) enligt vilken personuppgifter i det offentliga rättsinformationssystemet får föras över till tredjeland.

Enligt instruktionen för Bolagsverket får verket till tredjeland föra över personuppgifter i den utsträckning dessa ingår i de register verket för, i huvudsak publicitetsregister, t.ex. aktiebolagsregistret. En liknande reglering finns i Patent- och registreringsverkets instruktion. Dessa bestämmelser torde vara kopplade till möjligheten att föreskriva undantag enligt artikel 26.1 f för offentliga register.

Det finns även bestämmelser om undantag från förbudet i 33 § PuL i författningar som inte är regelrätta registerförfattningar eller informationshanteringsförfattningar utan hör till den kategori som vi i vår inventering kategoriserat som annan slags författning med inslag av dataskyddsbestämmelser, se avsnitt 4.2. En sådan bestämmelse är 12 § lagen (2006:1570) om skydd mot internationella hot mot människors hälsa enligt vilken Socialstyrelsen under vissa förhållanden har en sekretessbrytande skyldighet att informera Världshälsoorganisationen. För att uppfylla den uppgiftsskyldigheten får personuppgifter överföras till organisationen och tredjeland. Ett annat exempel är 3 § förordningen (2000:1222) om internationellt tullsamarbete enligt vilken Tullverket får, utan hinder av 33 § PuL, överföra personuppgifter till tredjeland om det behövs för att uppfylla skyldigheter som följer av internationella överenskommelser med annan stat eller mellanfolklig organisation som Sverige har tillträtt eller annars är förpliktat att följa.

12.4 Sekretess och överföring till tredjeland m.m.

En överföring av personuppgifter från en myndighet till mottagare i tredjeland innefattar också ett ”utlämnande” så som det begreppet används i bl.a. offentlighets- och sekretesslagen, se t.ex. 6 kap. 1 § om utlämnande av allmän handling och 6 kap. 4 § OSL om utlämnande av uppgift. En fråga av intresse här är hur bestämmelserna och begränsningarna i fråga om förutsättningarna för att överföra personuppgifter till tredjeland förhåller sig till frågan om offentlighet och sekretess.

Bestämmelserna i 33–35 §§ PuL är formellt neutrala i den meningen att det principiellt sett inte gör någon skillnad för bestämmelsernas tillämplighet huruvida personuppgifter som överförs omfattas av sekretess eller inte hos den utlämnande myndigheten. Det är en annan sak att eventuell sekretess för överförda personuppgifter givetvis kan påverka vilken skyddsnivå i mottagarlandet som bedöms krävas i det enskilda fallet.

Frågan om sekretess har däremot avgörande betydelse för vad som bedöms utgöra ett tillåtet eller otillåtet utlämnande till mottagare i tredjeland utifrån bestämmelserna om handlingsoffentlighet i 2 kap. TF.

Om personuppgifter (och övriga uppgifter) i en allmän handling är offentliga – dvs. inte omfattas av någon sekretessbestämmelse eller omfattas i och för sig men vid en prövning i det enskilda fallet bedöms inte vara sekretessbelagda – ska handlingen lämnas ut till enskild mottagare som begärt att få ta del av handlingen med stöd av 2 kap. TF. Detta gäller oavsett om mottagaren befinner sig i tredjeland. En utlänning är i princip likställd med en svensk medborgare (14 kap. 5 § andra stycket TF). Det innebär att en utlänning i tredjeland har samma rätt som svenska medborgare att mot fastställd avgift få en kopia av handlingen (2 kap. 13 § TF). Personuppgiftslagens regler ska inte tillämpas i den mån det skulle inskränka en myndighets skyldighet enligt 2 kap. TF att lämna ut uppgifter. Detta följer av grundlags företräde framför vanlig lag och av 8 § första stycket PuL. I praktiken betyder det att man inte kan neka ett utlämnande med hänvisning till att skyddsnivån i mottagarlandet inte är adekvat. I vilken mån utlämnandet i personuppgiftslagens mening utgör en överföring eller inte är alltså vid uttag med stöd av offentlighetsprincipen en akademisk fråga. Däremot kan skyddsnivån i mottagarlandet få betydelse för i vilken form utlämnandet sker. Myndigheterna är enligt tryckfrihetsförordningen inte skyldiga att lämna ut allmänna handlingar i elektronisk form. En begäran från utlandet kan således inte sällan antas komma att effektueras manuellt via pappersutskrifter som postas.

Vid utlämnande av personuppgifter till en mottagare i tredjeland i andra situationer än då 2 kap. TF aktualiserats, är regelverket dock inte lika tydligt. Handlar det om utlämnande på grund av någon författningsreglering för ärendehandläggning hos en myndighet eller liknande, t.ex. enligt förvaltningslagens bestämmelser om kommunikationsplikt eller parts rätt till insyn i ärendet (16 och 17 §§ FL), görs visserligen ingen skillnad på parter i Sverige, EU eller tredjeland. Det tycks emellertid inte finnas generellt tillämpliga bestämmelser som vare sig förpliktar eller begränsar myndigheter såvitt avser utlämnande av offentliga personuppgifter till mottagare i tredjeland, t.ex. en myndighet i ett sådant land. Den bestämmelse som finns i 6 kap. 5 § OSL, om att en myndighet på begäran av en annan myndighet är skyldig att lämna en uppgift som den förfogar över såvida uppgiften inte är sekretessbelagd, ses i allmänhet som en precisering av myndigheternas allmänna samverkansskyldighet enligt 6 § FL som tar sikte på svenska förvaltningsmyndigheter och dom-

stolar. Bestämmelsen i 6 kap. 5 § OSL medför alltså inte någon förpliktelse att lämna ut offentliga personuppgifter till utländska myndigheter (1982/83:KU12 s. 36) och en utländsk myndighet anses inte ha rätt att överklaga en myndighets beslut att inte lämna ut en allmän handling eller annars avslå en begäran om att få del av en personuppgiftuppgift (Lenberg m.fl., kommentaren till 6 kap. 7 §).

Utlämnande av sekretessbelagda uppgifter till utländsk myndighet eller mellanfolklig organisation får ske enligt 8 kap. 3 § OSL om utlämnandet sker i enlighet med särskild föreskrift i lag eller förordning eller annars om uppgiften i motsvarande fall skulle få lämnas ut till en svensk myndighet och det enligt den utlämnande myndighetens prövning står klart att det är förenligt med svenska intressen att uppgiften lämnas.

En särskild fråga som rör förhållandet mellan sekretess och överföringsförbudet i 33 § PuL gäller den s.k. PuL-sekretessen enligt 21 kap. 7 § OSL. Vi har i avsnitt 11.2.1 lämnat en utförlig redovisning av 21 kap. 7 § OSL i samband med frågan om utlämnande av personuppgifter i elektronisk form. Som har framgått där är det mottagarens tilltänkta behandling av personuppgifter som är av avgörande betydelse för bestämmelsens tillämplighet, inte huruvida myndighetens utlämnande utgör en behandling i strid med personuppgiftslagen.

Som redan framhållits kan överföringsförbudet i 33 § PuL alltså inte hindra ett utlämnande som sker enligt 2 kap. TF. Som vidare har framgått av avsnitt 11.2.1 kan, vid utlämnande på grund av 2 kap. TF av annars offentliga personuppgifter till mottagare i tredjeland, en tillämpning av sekretessbestämmelsen i 21 kap. 7 § OSL i de allra flesta fall inte innebära något hinder mot utlämnandet. Vid utlämnande till mottagare i tredjeland har personuppgifterna således inte samma sekretesskydd som vid utlämnanden till mottagare i Sverige. Däremot kan överföringsförbudet alltså i princip hindra att utlämnandet sker i elektronisk form eftersom man kan anta att det inte är lämpligt att lämna ut uppgifter i elektronisk form om skyddsnivån i mottagarlandet inte bedöms vara adekvat. Överföringsreglerna kan på så sätt ha en indirekt effekt.

Vad gäller annat utlämnande till enskilda mottagare och utländska myndigheter eller organisationer i tredjeland kan överföringsförbudet på motsvarande sätt utgöra ett hinder mot att personuppgifter lämnas ut i elektronisk form eller lämnas ut för att behandlas

elektroniskt i det tredjelandet. Detsamma gäller i fråga om utlämnande av ett manuellt register med personuppgifter eller av personuppgifter för manuell registerföring i tredjeland.

12.5 Våra överväganden och förslag

Förslag: Personuppgiftslagens bestämmelser om överföring av personuppgifter till tredjeland och föreskrifter eller beslut om undantag från förbudet att överföra personuppgifter till tredjeland som meddelats med stöd av 35 § PuL ska vara tillämpliga även vid myndigheters behandling av personuppgifter. Detta ska framgå av lagen genom en hänvisning till 33–35 §§ PuL.

I lagen införs därutöver ytterligare undantag för överföring av personuppgifter till tredjeland som saknar adekvat skyddsnivå, nämligen om

a) överföringen krävs för handläggningen av ett visst ärende, eller

b) överföringen är nödvändig för att fullgöra en uppgiftsskyldighet som följer av lag eller förordning eller avtal med annan stat eller mellanfolklig organisation som Sverige har tillträtt eller annars är förpliktat att följa.

Flertalet svenska myndigheters personuppgiftsbehandling avser i allt väsentligt personer som är bosatta eller annars verksamma här. Vissa myndigheter har i sin verksamhet emellertid behov av att kunna kommunicera och utbyta information med aktörer av olika slag utomlands, ofta med andra stater inom EU/EES-området. Men det kan antas att det inom i princip varje statlig eller kommunal myndighet kan uppstå en situation då frågan om överföring av personuppgifter till tredjeland kan bli aktuell, både i samband med handläggning av ärenden eller i annan verksamhet.

Dataskyddsdirektivets regler om överföring till tredjeland bör ses mot den bakgrunden att det såvitt avser enskilda aktörer utan det grundläggande överföringsförbudet inte skulle gälla någon begränsning i syfte att skydda enskildas integritet mot okontrollerad spridning av personuppgifter till länder som kanske helt saknar skydd för uppgifterna. På myndighetsområdet är emellertid förhållandet ett annat. Genom reglerna om tystnadsplikt och sekretess i offentlig-

hets- och sekretesslagen kan lagstiftaren sektors- eller myndighetsvis sägas redan ha tagit ställning till behovet av integritetsskydd. I den mån uppgifter är sekretessbelagda uppstår alltså normalt sett inget ”överföringsproblem” eftersom utgångspunkten såvitt avser enskilda mottagare är att sådana uppgifter inte ska lämnas ut. Huvudregeln beträffande utländska myndigheter och mellanfolkliga organisationer är också att sekretessbelagda uppgifter inte får röjas även om det finns vissa undantag (jfr 8 kap. 3 § OSL).

Det är alltså främst beträffande sådan överföring som inte sker som ett resultat av ett offentlighetsuttag, som avser icke sekretessbelagda personuppgifter och som sker till mottagare utanför EU/EES som det finns anledning att närmare överväga hur överföringsreglerna i personuppgiftslagen ska hanteras för myndigheternas vidkommande. Som exempel på en sådan situation kan nämnas att en myndighet använder sig av ett it-stöd som tillhandahålls och administreras av en leverantör som är etablerad i t.ex. USA eller Kina. Ett annat exempel kan vara när ett landsting använder sig av ett callcenter för tidsbokning inom sjukvården och det företag som tillhandahåller tjänsten är etablerat utanför Europa. Självfallet kan frågor om överföring till tredjeland även uppstå i den löpande ärendehandläggningen.

Personuppgiftslagens grundläggande förbud och undantag bör gälla

Dataskyddsdirektivet innebär ett krav på reglering av överföring av personuppgifter till tredjeland. Vid myndigheters behandling av personuppgifter gäller som har framgått normalt personuppgiftslagens bestämmelser om detta och de föreskrifter som meddelats enligt 35 § PuL. Särbestämmelser i registerförfattningar eller annan lagstiftning förekommer sällan. Vi ser ingen anledning att ändra på detta förhållande. Vi föreslår därför att bestämmelserna i personuppgiftslagen om överföring av personuppgifter till tredjeland ska vara tillämpliga även vid myndigheters behandling av personuppgifter enligt den nya lagen. Detta ska framgå genom en hänvisning i lagen till bestämmelserna i personuppgiftslagen. Även de föreskrifter och beslut som meddelats enligt 35 § PuL bör gälla enligt den nya lagen.

Såvitt avser enstaka överföringar av personuppgifter som behandlas i löpande text eller annars i ostrukturerat material, t.ex. i en e-postkommunikation, är, som vi har berört ovan, skyddsbehovet ofta så litet att även fullständig frånvaro av dataskyddsregler kan anses godtagbart. Skyddsnivån är adekvat eftersom det inte behövs något egentligt skydd för uppgifterna i fråga. Överföringsförbudet gäller i så fall inte. Vi har emellertid uppfattat det som att myndigheterna ändå ofta lutar sig mot missbruksregeln i 5 a § för att inte träffas av förbudet enligt 33 §. Något ställningstagande i fråga om vad som följer av 33 och 34 §§ eller föreskrifter som meddelats enligt 35 § görs då inte, utan bara prövningen om överföringen innebär en kränkning av den registrerades personliga integritet (5 a § andra stycket). Ett uppgiftsutlämnande får givetvis inte heller strida mot offentlighets- och sekretesslagen.

Vi har behandlat missbruksregeln i avsnitt 8.3 och föreslagit att den bestämmelsen eller någon motsvarighet till den inte bör gälla enligt den nya lagen. I det sammanhanget har vi framhållit att syftet med missbruksregeln inte har varit att underlätta myndigheternas behandling av personuppgifter utan att skapa en enklare och mindre byråkratisk reglering för enskilda och tillgodose deras rätt till yttrande- och informationsfrihet. Mot den bakgrunden är det enligt vår mening alltså inte tillfredsställande att myndigheter åberopar missbruksregeln för att finna lagstöd till att överföra personuppgifter till en mottagare i tredjeland. Inte heller ser vi något praktiskt behov av att i den nya lagen införa någon motsvarande lättnad för överföring av personuppgifter i s.k. ostrukturerat material. Som vi redan har konstaterat innebär överföringsbestämmelserna normalt sett inget hinder mot överföringar av sådana personuppgifter. En tillämpning av 33 § PuL leder alltså normalt till att personuppgifter i löpande text och liknande kan överföras även till tredjeland utan att träffas av personuppgiftslagens förbud. Vad gäller överföring av personuppgifter i strukturerat material får dock göras en bedömning av om det finns någon adekvat skyddsnivå eller om något annat undantag är tillämpligt. I samtliga fall krävs dessutom att överföringen till det tredjelandet sker för ett korrekt ändamål och uppfyller de övriga grundläggande kraven i 9 § samt är nödvändig för att myndigheten ska kunna utföra sin verksamhet.

Behov av ytterligare undantag

Bestämmelserna i 33 § PuL om att det ska göras bedömningar av om det utifrån omständigheterna finns adekvat skyddsnivå tycks vara utformade för situationer där det finns ett gott faktaunderlag om förhållandena i det tredjelandet och där det handlar om en planerad överföring av en omfattande mängd personuppgifter, vilket i sig ger anledning till särskilt samlade och övertänkta ställningstaganden. För den typen av överföringar är bestämmelserna ändamålsenligt utformade.

I en myndighets dagliga verksamhet med t.ex. ärendehantering torde det i realiteten vara tämligen vanskligt att göra den typen av bedömningar för varierande situationer, personuppgiftskategorier och olika mottagarländer. Till saken hör även att kommissionens beslut om adekvat skyddsnivå i vissa länder endast omfattar ett förhållandevis begränsat antal stater eller mottagare.

Samtycke från berörda registrerade är inte ett undantag som kan fungera tillfredsställande i myndigheters verksamhet. Om t.ex. en inlaga ska kommuniceras med en part, så skulle det inte räcka med att inhämta dennes samtycke. Andra i inlagan eventuellt omnämnda personer måste också kontaktas och tillfrågas. Ett sådant förfarande är inte förenligt med att myndigheterna måste ha förutsättningar att sköta sina uppgifter på ett rationellt och effektivt sätt.

Övriga undantag som föreskrivs i 34 § PuL är inte heller helt anpassade för myndigheternas behov eller allmänhetens förväntningar. Visserligen torde bestämmelsen i 34 § första stycket c – på motsvarande sätt som undantaget i 16 § första stycket c PuL i fråga om känsliga personuppgifter – kunna ge ett visst utrymme för en handläggande myndighet att i vissa sorters ärenden trots förbudet i 33 § första stycket överföra personuppgifter till tredjeland som saknar adekvat skyddsnivå. Vi bedömer dock att det undantaget, som förefaller tämligen oklart till sin räckvidd, inte fyller det generella behov som kan finnas hos alla myndigheter att i ett enskilt fall kunna överföra personuppgifter till tredjeland.

De behov av ytterligare undantag som vi identifierat tar sikte på två olika situationer.

För det första måste myndigheter på ett rättssäkert och effektivt sätt kunna handlägga ärenden med användning av modern teknik för att kommunicera och kunna förmedla information även till

enskilda som befinner sig i avlägsna länder. Vi menar att överföring av personuppgifter som krävs för handläggning av ett visst ärende uppfyller direktivets krav på att utgöra ett viktigt allmänt intresse (artikel 26.1 d) för vilket medlemsstater får föreskriva undantag i nationell rätt. Vi föreslår därför ett sådant undantag. När det gäller överföring av personuppgifter utanför ramen för en myndighets ärendehandläggning ser vi däremot inget behov av ett generellt undantag.

Det andra behovet av undantag är föranlett av att myndigheter kan ha uppgiftsskyldighet i förhållande till myndigheter i tredjeland eller till internationella organisationer. Om det är nödvändigt för en myndighet att överföra uppgifter till tredjeland för att fullgöra en uppgiftsskyldighet i lag eller förordning eller en internationell överenskommelse som är bindande för Sverige, finns det uppenbarligen ett viktigt allmänt intresse av att myndigheten kan fullgöra denna skyldighet med användning av modern informationsteknik utan hinder av överföringsförbudet enligt 33 § PuL. Detsamma gäller i fråga om uppgifter för vidare bearbetningar utomlands. Mot den bakgrunden föreslår vi ett generellt undantag för uppgiftsskyldigheter av det slaget. En förutsättning för att undantaget ska vara tillämpligt är dock att det är nödvändigt att överföra personuppgifterna. Kan uppgiftsskyldigheten fullgöras utan personuppgifter eller med anonymiserade uppgifter, är nödvändighetsrekvisitet inte uppfyllt. Vidare måste överföringen ske med godtagbar säkerhet till skydd för uppgifterna. Såvitt avser sekretessbelagda personuppgifter måste det vidare självfallet vara fråga om ett tillåtet utlämnande enligt offentlighets- och sekretesslagen, jfr 8 kap. 3 § OSL angående utlämnande till utländska myndigheter eller mellanfolkliga organisationer. Är det fråga om en särskilt föreskriven uppgiftsskyldighet i lag eller förordning följer av 8 kap. 3 § första punkten att sekretess inte hindrar ett utlämnande. Med lag eller förordning likställs en EU-förordning. Är det fråga om en skyldighet att överföra uppgifter till följd av ett internationellt avtal som är bindande för Sverige får en prövning göras enligt andra punkten i samma paragraf enligt vilken sekretess inte utgör något hinder om uppgiften i motsvarande fall skulle få lämnas ut till en svensk myndighet och det enligt den utlämnande myndighetens prövning står klart att det är förenligt med svenska intressen att uppgiften lämnas till den utländska myndigheten eller den mellanfolkliga organisationen.

En prövning enligt andra punkten i fall som nu avses torde som regel utmynna i bedömningen att personuppgifterna i fråga kan lämnas ut utan hinder av sekretess.

Internetpublicering

Vi delar E-offentlighetskommitténs bedömning att EU-domstolens dom i det s.k. konfirmandmålet måste förstås på det sättet att publicering av uppgifter på internet i de allra flesta fall inte innebär överföring till tredjeland i dataskyddsdirektivets mening. Något undantag från 33 § PuL är därför inte påkallat för att tillgodose myndigheternas behov av internetpubliceringar. Huruvida en viss internetpublicering utgör en tillåten behandling enligt de grundläggande kraven i 9 § PuL är en helt annan sak.

13 Information till den registrerade

13.1 Allmänna dataskyddsrättsliga regler

Dataskyddsdirektivet

Att en registrerad kan få information om och insyn i behandlingar av personuppgifter om honom eller henne är en förutsättning för att han eller hon ska kunna kontrollera om behandlingen är lagenlig och i övrigt ta tillvara sina intressen och rättigheter. Direktivet innehåller därför bestämmelser om både skyldigheter för personuppgiftsansvariga att självmant informera och rättigheter för registrerade att få information.

Bestämmelserna om information som registeransvariga självmant ska lämna till den registrerade finns i artiklarna 10 och 11. Medlemsstaterna har frihet att föreskriva en vidare informationsplikt än vad som följer av artikel 10 eller 11 i direktivet, som i dessa avseenden är minimikrav. Artiklarna talar alltså om vad personuppgiftsansvariga i vart fall eller åtminstone måste informeras om. Bestämmelserna om den registrerades rätt att på begäran få information från den registeransvarige finns i artikel 12 a. Generella möjligheter till begränsningar i skyldigheterna respektive rättigheterna anges i artikel 13. Dessutom görs vissa undantag direkt i artiklarna 10 och 11.

Artikel 10 reglerar informationsplikten i samband med att personuppgifter samlas in från den registrerade själv. Medlemsstaterna åläggs att föreskriva att han eller hon då i vart fall ska få information om följande.

a) Den registeransvariges och dennes eventuella företrädares identitet.

b) Ändamålen med den behandling för vilken uppgifterna är avsedda.

c) All ytterligare information, exempelvis

- mottagarna eller de kategorier som mottar uppgifterna,
- huruvida det är obligatoriskt eller frivilligt att besvara frågorna samt eventuella följder av att inte svara,
- förekomsten av rättigheter att få tillgång till och att erhålla rättelse av uppgifter som rör honom,

i den utsträckning som den ytterligare informationen – med hänsyn till de särskilda omständigheter under vilka uppgifterna samlas in – är nödvändig för att tillförsäkra den registrerade en korrekt behandling.

Information enligt artikel 10 behöver dock inte lämnas om den registrerade redan känner till informationen.

Artikel 11 reglerar informationsplikten när behandlade uppgifter inte har samlats in från den registrerade. Av bestämmelsen följer att medlemsstaterna ska föreskriva att den registeransvarige då ska lämna den registrerade samma information som anges i artikel 10 a, b och c dock att, beträffande den ytterligare information som ska ges enligt punkten c, information ska ges om de kategorier av uppgifter som behandlingen gäller i stället för huruvida det är obligatoriskt eller frivilligt att besvara frågor. Informationen ska lämnas vid tiden för registreringen av personuppgifter eller, om utlämnande till en tredje man kan förutses, inte senare än vid den tidpunkt då uppgifterna först lämnas ut.

Inte heller enligt artikel 11 behöver information lämnas om det som den registrerade redan känner till. Dessutom gäller att information inte behöver lämnas när det visar sig vara omöjligt eller innebär en oproportionerligt stor ansträngning att ge information. Information behöver inte heller ges om registreringen eller utlämnandet uttryckligen föreskrivs i författning. Detta gäller särskilt i samband med behandling för statistiska ändamål eller historiska eller vetenskapliga forskningsändamål. I sådana fall ska medlemsstaterna föreskriva lämpliga skyddsåtgärder (artikel 11.2). Enligt punkten 40 i ingressen till direktivet kan i detta sammanhang antalet registrerade, uppgifternas ålder och de kompensatoriska åtgärder som kan vidtas tas i beaktande.

Artikel 12 a anger att medlemsstaterna ska säkerställa att varje registrerad har rätt att från den registeransvarige

– få bekräftelse på om uppgifter som rör honom behandlas eller inte och information om åtminstone ändamålen med behandlingen, de berörda uppgiftskategorierna och mottagarna eller mottagarkategorierna till vilka uppgifterna utlämnas,
– få begriplig information om vilka uppgifter som behandlas och all tillgänglig information om varifrån dessa uppgifter kommer,
– få kännedom om den logik som används när uppgifter som rör honom behandlas på automatisk väg åtminstone såvitt avser sådana automatiska beslut som avses i artikel 15.1.

Detta ska ske med rimliga intervall samt utan större tidsutdräkt eller kostnader.

Medlemsstaterna får genom lagstiftning vidta åtgärder för att begränsa de registeransvarigas skyldigheter och de registrerades rättigheter enligt artiklarna 10–12. Förutsättningarna för detta anges i artikel 13. Det krävs att begränsningarna är en nödvändig åtgärd med hänsyn till a) statens säkerhet, b) försvaret, c) allmän säkerhet, d) förebyggande, undersökning, avslöjande av brott eller åtal för brott eller av överträdelser av etiska regler som gäller för lagreglerade yrken, e) ett viktigt ekonomiskt eller finansiellt intresse hos en medlemsstat eller hos Europeiska unionen, inklusive monetära frågor, budgetfrågor och skattefrågor, f) en tillsyns-, inspektions- eller regleringsfunktion som, även om den är av övergående karaktär, är förbunden med myndighetsutövning i de under punkterna c, d och e nämnda fallen, eller g) skydd av den registrerades eller andras fri- och rättigheter.

Dessutom får medlemsstaterna, i synnerhet om uppgifterna inte används för åtgärder eller beslut som avser särskilda registrerade personer, i fall då det uppenbarligen inte föreligger någon risk att den berörda personens privatliv kränks, genom lagstiftning begränsa de rättigheter som anges i artikel 12 när uppgifterna endast behandlas för ändamål som har med vetenskaplig forskning att göra eller när uppgifterna endast lagras i form av personuppgifter under en begränsad tid som inte överstiger den tid som är nödvändig för att framställa statistik (artikel 11.2). Möjligheten till begränsningar enligt denna punkt förutsätter dock lämpliga rättsliga garantier.

Personuppgiftslagen

Bestämmelserna i artiklarna 10–12 rörande information har genomförts i svensk lagstiftning genom 23–26 §§ PuL. Bestämmelserna följer i stort direktivets disposition och innehåll.

Samtliga paragrafer hör till dem som räknas upp i den s.k. missbruksregeln i 5 a § första stycket PuL. De behöver alltså inte tillämpas vid behandling av personuppgifter som inte ingår i eller är avsedda att ingå i en samling av personuppgifter som har strukturerats för att påtagligt underlätta sökning eller sammanställning av personuppgifter, s.k. ostrukturerat material.

Bestämmelserna i 23–26 §§ PuL gäller inte i den utsträckning det är särskilt föreskrivet i lag eller annan förordning eller i beslut som har meddelats med stöd av författning att uppgifter inte får lämnas ut till den registrerade. Detta följer av 27 § PuL. För myndigheters del är det bestämmelser i offentlighets- och sekretesslagen som åsyftas, dvs. bestämmelser som innebär hinder mot att personuppgifter röjs på grund av sekretess. Sekretess till skydd för enskilda gäller inte gentemot den enskilde själv annat än i rena undantagsfall (12 kap. 1 § OSL). Det innebär i praktiken att sekretess begränsar informationsskyldigheten enligt 23–26 §§ PuL bara i fråga om uppgifter som omfattas av sekretess till skydd för det allmännas intresse, t.ex. sekretess för uppgifter till skydd för brottsbekämpningen, eller avser ett sekretesskyddat intresse hos någon annan enskild än den registrerade.

Enligt 50 § e PuL meddelar regeringen, eller myndighet som regeringen bestämmer, närmare föreskrifter om vilken information som ska lämnas till den registrerade och hur informationen ska lämnas. Datainspektionen har genom 16 § PuF bemyndigats att meddela sådana föreskrifter. Några föreskrifter har dock inte meddelats. Däremot har inspektionen utfärdat allmänna råd om information till registrerade.

Information som den personuppgiftsansvarige ska lämna självmant

Bestämmelserna i 23–25 §§ PuL motsvarar artiklarna 10 och 11 i dataskyddsdirektivet. I förarbetena anmärktes att dessa artiklar måste genomföras i svensk lagstiftning och att det borde ske genom att bestämmelserna fördes över till personuppgiftslagen, som alltså

inte går längre än vad som krävs enligt direktivet (prop. 1997/98:44 s. 79).

I 23 § PuL föreskrivs att om uppgifter om en person samlas in från personen själv, ska den personuppgiftsansvarige i samband därmed självmant lämna den registrerade information om behandlingen av uppgifterna.

Om personuppgifterna har samlats in från någon annan källa än den registrerade, ska, enligt 24 § första stycket PuL, den personuppgiftsansvarige självmant lämna den registrerade information om behandlingen av uppgifterna när de registreras. Är uppgifterna avsedda att lämnas ut till tredje man, behöver informationen dock inte ges förrän uppgifterna lämnas ut för första gången. Enligt 24 § andra stycket behöver information dock inte lämnas, om det finns bestämmelser om registrerandet eller utlämnandet av personuppgifterna i en lag eller någon annan författning. För att detta undantag ska vara tillämpligt, krävs att författningsregleringen uttryckligen tar sikte på registrering eller utlämnande av personuppgifter, se artikel 11.2 i direktivet. Tanken bakom undantaget är att den registrerade har möjlighet att genom att ta del av författningen få kännedom om vad som kan komma att hända med uppgifterna. I Datainspektionens allmänna råd om information till registrerade anges att myndigheters registrering av allmänna handlingar enligt 5 kap. 1 och 2 §§ OSL omfattas av undantaget. Datalagskommittén anförde att bestämmelser om arkivmyndigheters omhändertagande av arkivmaterial är tillräckligt preciserade för att omfattas av det nämnda undantaget (SOU 1997:39 s. 388). I 24 § tredje stycket PuL föreskrivs vidare att information enligt första stycket inte behöver lämnas, om detta visar sig vara omöjligt eller skulle innebära en oproportionerligt stor arbetsinsats. Om uppgifterna används för att vidta åtgärder som rör den registrerade, ska dock information lämnas senast i samband med att så sker.

I 25 § första stycket PuL anges närmare vad information enligt 23 eller 24 § ska innehålla, nämligen följande.

a) uppgift om den personuppgiftsansvariges identitet,

b) uppgift om ändamålen med behandlingen, och

c) all övrig information som behövs för att den registrerade ska kunna ta till vara sina rättigheter i samband med behandlingen, såsom information om mottagarna av uppgifterna, skyldighet att lämna uppgifter och rätten att ansöka om information och få rättelse.

Det har alltså inte meddelats några föreskrifter om hur information enligt 23 eller 24 § ska lämnas, utan det är en fråga som i hög grad beror på omständigheterna i det enskilda fallet. Vägledning finns i Datainspektionens allmänna råd. Där lämnas bl.a. rekommendationer om hur information bör ges när uppgifter samlas in muntligen, via blanketter, via loggning då internet används m.m.

En viktig begränsning i informationsskyldigheten enligt 23 och 24 §§ är att information inte behöver lämnas om sådant som den registrerade redan känner till (25 § andra stycket PuL). Det är ett undantag som har stor relevans för myndigheters behandling av personuppgifter. I förarbetena uttalades att eftersom utlämnande av allmänna handlingar enligt offentlighetsprincipen sedan lång tid tillbaka föreskrivits i svensk grundlag, kan det förutsättas att allmänheten redan känner till att så kan ske. Därför torde det inte vara nödvändigt att lämna särskild information i det hänseendet (prop. 1997/98:44 s. 44 f.). Däremot kan givetvis information lämnas om att uppgifterna kan komma att lämnas ut enligt 2 kap. TF till var och en som begär det.

Datainspektionen framhåller i sina allmänna råd att den registrerade under vissa förutsättningar får anses känna till behandlingen även om någon information inte har lämnats av den personuppgiftsansvarige eller någon annan. Om den registrerade själv har lämnat in personuppgifter till den personuppgiftsansvarige, t.ex. genom att till en kommun lämna in en ansökan om ekonomiskt bistånd, behöver kommunen inte lämna information så länge uppgifterna bara behandlas för de ändamål som den registrerade kan förutse. I en sådan situation får den registrerade anses känna till den personuppgiftsansvariges identitet och ändamålen med behandlingen. Det får också anses att den registrerade under nämnda förutsättning inte är i behov av ytterligare information för att kunna ta tillvara sina rättigheter.

I sammanhanget bör nämnas att de principer om parts rätt till insyn i ärenden och myndigheternas skyldighet att se till att parten får del av uppgifter som tillförts ett ärende av annan än parten själv

medför att registrerades behov av insyn i personuppgiftsbehandlingen i praktiken ofta tillgodoses genom förfaranderegleringar som gäller i mål- och ärendehantering hos domstolar och myndigheter. Centrala bestämmelser om rätten till partsinsyn och myndigheters kommunikationsplikt finns i 16 och 17 §§ FL. Motsvarande rätt till insyn och skyldigheter att självmant kommunicera uppgifter med parter finns i de processuella regelverken, se t.ex. 10–12, 18, 19 och 43 §§ FPL eller 22 § lagen (1996:242) om domstolsärenden. Motsvarande följer även av rättegångsbalken. Rätten till insyn och skyldigheten att kommunicera uppgifter enligt förfaranderegleringarna är mer vidsträckt än enligt personuppgiftslagens informationsregler genom att de inte annat än i undantagsfall kan begränsas på grund av sekretess, se 10 kap. 3 § OSL.

Information som ska lämnas efter ansökan

Bestämmelserna i 26 § första stycket PuL handlar om information som den personuppgiftsansvarige är skyldig att lämna efter ansökan från den registrerade. Enligt bestämmelserna ska var och en som ansöker om det en gång per kalenderår lämnas gratis besked om personuppgifter som rör den sökande behandlas eller inte.

Behandlas sådana uppgifter, ska dessutom skriftlig information lämnas om

a) vilka uppgifter om den sökande som behandlas,

b) varifrån dessa uppgifter har hämtats,

c) ändamålen med behandlingen, och

d) till vilka mottagare eller kategorier av mottagare som uppgifterna lämnas ut.

Det ska observeras att det i 26 § inte finns någon motsvarande begränsning som i 25 § beträffande uppgifter som den registrerade redan känner till. Även sådan information ska alltså lämnas. Det kan t.ex. innebära att information måste omfatta uppgifter som den registrerade redan har fått del av i ett numera avgjort ärende på grund av ovan nämnda bestämmelser i förvaltningslagen om kommunikationsplikt m.m. i det då pågående förfarandet.

När det gäller information om varifrån uppgifterna kommer, punkt b, behöver den personuppgiftsansvarige bara lämna den information som finns tillgänglig för denne. Den personuppgiftsansvarige behöver alltså inte hålla reda på varifrån uppgifterna har hämtats, men vet den personuppgiftsansvarige det när den registrerade ansöker om information ska det uppges (prop. 1997/98:44 s. 81 f.).

När det gäller punkten d kan man utgå från att personuppgiftslagen inte kräver att myndigheter dokumenterar utlämnande till mottagare som begärt insyn enligt 2 kap. TF. Det är nämligen inte förenligt med det s.k. frågeförbudet enligt 2 kap. 14 § TF att myndigheter vid offentlighetsuttag dokumenterar vilka mottagare som fått del av allmänna handlingar med personuppgifter. Däremot bör i informationen allmänt anges att uppgifterna kan komma att lämnas ut enligt offentlighetsprincipen till den som begär det, i den mån de inte är sekretessbelagda (jfr prop. 1997/98:44 s. 45).

Datainspektionen framhåller i sina allmänna råd att avsikten är att den personuppgiftsansvarige från sina register eller andra samlingar av personuppgifter ska lämna ett utdrag med alla de upplysningar som är att anse som personuppgifter beträffande den registrerade. När personuppgifter behandlas automatiserat ska alltså enligt Datainspektionen information om vilka uppgifter som behandlas ges genom att den registrerade erhåller en datautskrift. När det gäller manuell behandling av personuppgifter ska information i stället lämnas genom att den registrerade erhåller en kopia av de personuppgifter som finns i det manuella registret.

En ansökan om information kan inte göras formlöst. Det krävs att ansökan görs skriftligen hos den personuppgiftsansvarige. Ansökan ska vara undertecknad av den sökande själv (26 § andra stycket första meningen PuL). Enligt Datainspektionens allmänna råd medför det att ansökan måste göras per pappersskrift. Det viktiga i sammanhanget torde vara att på något sätt kunna kontrollera att begäran verkligen härrör från den registrerade själv. Något vägledande avgörande om att ansökan bara kan göras per pappersskrift eller om en kvalificerad elektronisk signatur skulle kunna vara godtagbar finns inte.

Informationen ska lämnas inom en månad från det att ansökan gjordes. Om det finns särskilda skäl för det, får informationen lämnas senare, dock senast fyra månader efter det att ansökan gjordes

(26 § andra stycket andra och tredje meningarna PuL). Sådana särskilda skäl kan vara att personuppgifterna är krypterade, att sökmöjligheterna annars är begränsade eller att den personuppgiftsansvarige har många personuppgifter uppdelade på olika register eller andra datasamlingar (prop. 1997/98:44 s. 132).

Föreskrifterna i 26 § första stycket PuL avses genomföra artikel 12 a i dataskyddsdirektivet. Samtidigt finns inslag i bestämmelsen som härrör från en motsvarande bestämmelse om registerutdrag som fanns i 10 § datalagen (1973:289). Kravet på skriftlig och egenhändigt undertecknad ansökan är ett sådant inslag. Likaså ettårsbegränsningen och huvudregeln om enmånadsfristen för när utdraget ska lämnas. Än i dag är det vanligt att information enligt 26 § PuL kallas för registerutdrag, vilket är en missvisande benämning eftersom personuppgiftslagen, och därmed informationsplikten, till skillnad från datalagen omfattar mer än bara personuppgifter som behandlas i register.

I förarbetena angavs att det är rimligt att utgå från att regleringen i 26 § PuL inte innebär mer än att den personuppgiftsansvarige är skyldig att utnyttja alla de sök- och sammanställningsmöjligheter som han eller hon har tillgång till för att få fram information att lämna till den registrerade (prop. 1997/98:44 s. 82 f.). Regeringen anslöt sig därmed till vad Datalagskommittén hade anfört (SOU 1997:39 s. 392 f.). Enligt kommittén var det inte rimligt att informationsskyldigheten skulle utformas på ett sådant sätt att den tvingar fram förfaranden som i själva verket kan hota den personliga integriteten. Den personuppgiftsansvarige bör, som kommittén såg det, bara vara skyldig att utnyttja alla de sök- och sammanställningsmöjligheter som han eller hon faktiskt och rättsligt har tillgång till för att få fram information att lämna till den registrerade. Därmed garanteras att den registrerade får tillgång till all information som den personuppgiftsansvarige själv kan få fram om den registrerade. Vad som närmare kan ha avsetts med sök- och sammanställningsmöjligheter som en personuppgiftsansvarig har tillgång till framgår dock inte. Någon vägledande praxis om hur långtgående sökningar som måste göras finns inte heller.

I 26 § tredje stycket PuL finns dock ett visst begränsat undantag. Enligt den bestämmelsen behöver den personuppgiftsansvarige inte informera om personuppgifter i löpande text som inte fått sin slutliga utformning när ansökan gjordes eller som utgör minnes-

anteckning eller liknande. Information måste dock ändå ges i vissa fall, bl.a. om uppgifterna i den löpande texten har behandlats under längre tid än ett år. I förarbetena påpekade regeringen att informationsskyldigheten innebär att registrerade i vissa fall kan ha rätt att med stöd av personuppgiftslagen få ta del av uppgifter om sig själva som allmänheten inte har rätt att få ta del av med stöd av 2 kap. TF. Den registrerade har alltså i viss utsträckning rätt att ta del av uppgifter i handlingar som inte är allmänna, t.ex. personuppgifter i utkast som har behandlats under längre tid än ett år (prop. 1997/98:44 s. 83 f.).

Till skillnad från vad som gäller beträffande information enligt 23–25 §§ PuL kan en myndighets beslut rörande information enligt 26 § överklagas till allmän förvaltningsdomstol enligt 52 § PuL. Denna överklagandebestämmelse infördes vid 2006 års ändringar av personuppgiftslagen. Även dessförinnan hade motsvarande överklagandebestämmelser förekommit i en del registerförfattningar.

Som allmän princip inom förvaltningsrätten gäller att det bara är sådana beslut som på ett eller annat sätt har gått den klagande emot som är överklagbara. Såvitt avser information enligt 26 § PuL torde detta normalt innebära att det enbart är beslut innebärande helt eller delvis avslag på en begäran som kan överklagas.

Rätten att överklaga en myndighets beslut om information enligt 26 § är en inhemsk reglering. Dataskyddsdirektivet ställer inget sådant krav. Vad direktivet dock kräver är en rätt att föra talan vid domstol. Se vidare om överklagande i avsnitt 18.3.

Missbruksregeln och 26 § PuL

Rätten till s.k. registerutdrag fanns alltså redan enligt 1973 års datalag. Från tid till annan har emellertid skyldigheten att lämna registerutdrag setts som betungande administrativt och ekonomiskt, se t.ex. Justitiedepartementets utvärdering av dataskyddsdirektivet enligt vilken många myndigheter tog upp registerutdragen som ett problem (Ds 2001:27 s. 75 f.).

Personuppgiftslagsutredningen tog mot den bakgrunden upp frågan om det var möjligt eller lämpligt att genom en ändring i personuppgiftslagen göra någon inskränkning i skyldigheten att lämna registerutdrag. Utredningen uttalade bl.a. följande (SOU 2004:6

s. 195 f.). Det som brukar anföras som särskilt betungande för personuppgiftsansvariga är att i vissa fall söka fram alla de personuppgifter om den registrerade som behandlas. Det gäller främst när en personuppgiftsansvarig har en större mängd ostrukturerat material, t.ex. i form av löpande text eller ljud- och bildupptagningar, särskilt om materialet finns på olika ställen, t.ex. i hundratals persondatorer. Men det gäller också när en personuppgiftsansvarig har väldigt många regelrätta register att söka igenom. Om den personuppgiftsansvarige bara efter väldigt stora ansträngningar kan få fram uppgifter om en person, är det mindre sannolikt att dessa uppgifter kommer att användas på ett sätt som innebär ett otillbörligt intrång i den personliga integriteten. Det kan i vart fall konstateras att informationsteknikens särskilda möjligheter att effektivt strukturera, söka och sammanställa uppgifter då inte har utnyttjats på ett sätt som innebär särskilda integritetsrisker. Av bl.a. detta skäl ansåg utredningen att det skulle vara befogat och inte innebära någon egentlig och beaktansvärd inskränkning av integritetsskyddet att i personuppgiftslagen ange att skyldigheten att lämna registerutdrag inte gäller i den utsträckning det visar sig vara omöjligt eller skulle innebära en oproportionerligt stor arbetsinsats att lämna utdrag. Enligt utredningen var ett sådant undantag förenligt med dataskyddsdirektivet. Däremot föreslogs inte att den samtidigt föreslagna missbruksregeln skulle omfatta även 26 §.

Regeringen gjorde en annan bedömning och anförde bl.a. följande (prop. 2005/06:173 s. 41).

> Det kan förvisso hävdas att en rätt att begära registerutdrag har betydelse för att den registrerade skall kunna kontrollera att hans personuppgifter inte behandlas i strid med missbruksregeln, dvs. missbrukas. Missbruksregeln är emellertid avsedd att träffa sådana behandlingar som typiskt sett inte innefattar några risker för intrång i den personliga integriteten. Det behov av kontroll som den registrerade kan ha kan inte anses förknippat med behandlingen som sådan – t.ex. att skriva ett namn i ett ordbehandlingsdokument – utan är snarare beroende av i vilket sammanhang personuppgifterna förekommer och av vilken spridning de kan få. I den mån det verkligen är fråga om ett missbruk av personuppgifter kommer detta i normalfallet att komma till den registrerades kännedom på annat sätt än genom ett registerutdrag, t.ex. genom Internetpublicering. Rätten att få registerutdrag en gång per kalenderår kan alltså enligt regeringens bedömning inte anses vara en förutsättning för att kränkningar av den personliga integriteten i enlighet med missbruksregeln skall kunna uppdagas och beivras. Sammanfattningsvis anser således regeringen att utdragsskyldighetens

värde från kontrollsynpunkt vid behandling av personuppgifter i ostrukturerat material inte är särskilt framträdande.

Missbruksregeln kom alltså att omfatta även 26 § PuL. Enligt regeringen borde det däremot inte göras någon ändring av skyldigheten att lämna information enligt 26 § PuL för sådana behandlingar som även fortsättningsvis skulle omfattas av lagens hanteringsregler. Regeringen anförde i denna del bl.a. följande (prop. 2005/06:173 s. 50). Rätten att på begäran få ett registerutdrag är grundläggande för den registrerade och har funnits alltsedan 1973 års datalag antogs. Den fyller en viktig kontrollfunktion, framför allt när uppgifterna finns i regelrätta register och stora databaser där integritetsriskerna typiskt sett är större. Genom registerutdraget får den registrerade möjlighet att kontrollera om han eller hon är registrerad och, om så är fallet, att de registrerade uppgifterna är riktiga. Rätten till insyn är vidare en förutsättning för att den registrerade i praktiken skall kunna få felaktiga uppgifter rättade i sådant material som inte omfattas av den föreslagna missbruksregeln.

Förslaget till uppgiftsskyddsförordning

Kommissionen

Förslaget till uppgiftsskyddsförordning bygger på dataskyddsdirektivets bestämmelser om vilken information som ska ges till den registrerade. Vissa tillkommande krav har dock föreslagits både vad gäller informationens innehåll (artiklarna 14 och 15) samt formerna för hanteringen och administrationen av informationsskyldigheten (artiklarna 11 och 12). De begränsningar i informationsplikten som får föreskrivas anges i artikel 21. Bestämmelserna finns i förordningens kapitel III med rubriken Den registrerades rättigheter.

I artikel 14 preciseras närmare den registeransvariges skyldighet att självmant informera den registrerade. De nuvarande kraven i artiklarna 10 och 11 i direktivet behålls. Dessutom ska den registrerade få information om kontaktuppgifter till uppgiftsskyddsombudet, lagringsperioden, rätten att inge ett klagomål till tillsynsmyndigheten samt, i tillämpliga fall, om att den registeransvariga avser överföra personuppgifterna till tredjeland eller en internationell organisation och nivån på det skydd som mottagaren kan er-

bjuda (14.1). När det gäller personuppgifter som inte samlas in från de registrerade ska information lämnas om var personuppgifterna har sitt ursprung (14.3). De möjliga undantagen enligt artiklarna 10 och 11 dataskyddsdirektivet finns kvar. Dessutom anges att när uppgifter inte samlas in från den registrerade, behöver information inte tillhandahållas om det får en negativ verkan på andras fri- och rättigheter på sätt som fastställs i unionslagstiftningen eller medlemsstatens lagstiftning enligt artikel 21 (14.5). Kommissionen föreslås kunna meddela genomförandeakter samt fastställa standardformulär för tillhandahållande av information (14.7 och 8).

I artikel 15 ges den registrerade en rätt till tillgång till sina personuppgifter. Artikel 15 motsvarar artikel 12 a i dataskyddsdirektivet, dock att det tydliggörs att det handlar om information som ska tillhandahållas på begäran. Vidare har det gjorts några tillägg i fråga om vad informationen ska omfatta. Exempelvis ska anges vilka mottagare i tredjeland som kan komma i fråga. Vidare ska lagringsperioden anges liksom rätten till rättelse och radering samt att inge ett klagomål till tillsynsmyndigheten. Om den registrerade gör en begäran i elektronisk form ska informationen också tillhandahållas i elektronisk form, om en registrerad inte begär något annat (15.2). Kommissionen föreslås få befogenhet att anta delegerade akter och standardformulär eller förfaranden, t.ex. för kontroll av den registrerades identitet (15.3 och 4).

I artiklarna 11 och 12 fastställs vissa allmänna krav på den registeransvarige som syftar till att främja den registrerades möjligheter att utöva sina rättigheter enligt förordningen, dvs. inte bara rätten till information utan även rätten till t.ex. rättelse, radering och att göra invändningar. Enligt artikel 11 gäller en skyldighet för registeransvariga att tillhandahålla klar och tydlig samt lätt tillgänglig policy för behandlingen av personuppgifter och för utövandet av den registrerades rättigheter. Information till registrerade ska vara begriplig och anpassad till den registrerade, i synnerhet i fråga om eventuell information till barn.

Av artikel 12 följer att en registeransvarig måste införa förfaranden och rutiner som den registrerade kan använda för att utöva sina rättigheter, bl.a. i fråga om att tillhandahålla information självmant enligt artikel 14 eller på begäran enligt artikel 15. Registeransvariga måste, som huvudregel, inom en månad underrätta den registrerade om vidtagna åtgärder med anledning av begäran om information

enligt artikel 15. Om den registeransvarige vägrar att vidta åtgärder på den registrerades vägnar, ska den registeransvarige informera den registrerade om orsaken och om möjligheten att lämna in ett klagomål till tillsynsmyndigheten och begära rättslig prövning (12.3). Den information och de åtgärder som vidtas på begäran ska vara gratis. Avgift får dock tas ut om begäran är uppenbart orimlig, särskilt på grund av dess repetitiva karaktär. Kommissionen föreslås få anta delegerade akter och fastställa standardformulär m.m. (12.5 och 6).

Från kraven enligt de nämnda artiklarna om den registeransvariges informationsskyldigheter finns vissa möjligheter till begränsningar. Detta föreskrivs i artikel 21 som i princip motsvarar artikel 13 i dataskyddsdirektivet. Skillnaderna gentemot direktivet är dels att begränsningar får föreskrivas både i unionsrätt och i medlemsstaternas lagstiftning, dels att begränsningen för allmänna intressen inte är avgränsad till ekonomiska eller finansiella intressen, såsom enligt direktivet, utan kan även avse andra allmänna intressen, dock att det anges särskilt ett av unionens eller en medlemsstats viktiga ekonomiska eller finansiella intressen (21.1 c jfr artikel 13.1. e i direktivet).

Utöver dessa bestämmelser föreslås i artikel 32 en helt ny informationsplikt, nämligen information som i vissa fall ska ges den registrerade om ”inträffade personuppgiftsbrott”. Med personuppgiftsbrott avses ett säkerhetsbrott som leder till förstöring, förlust eller ändringar genom olyckshändelse eller otillåtna handlingar eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats (artikel 4.9).

Europaparlamentet

Europaparlamentet har i sin resolution med ändringsförslag i uppgiftsskyddsförordningen framför allt föreslagit olika tillägg i bestämmelserna om informationsplikt enligt artiklarna 12, 14 och 15. Dessutom har parlamentet, i linje med övriga förslag till förändringar i uppgiftsskyddsförordningen, föreslagit att Kommissionens befogenheter att anta delegerade akter och standardformulär m.m. utgår.

Vad gäller artikel 12 har parlamentet föreslagit att registeransvariga om möjligt ska erbjuda registrerade fjärråtkomst där den registrerade får direkt tillgång till sina personuppgifter.

Vidare har parlamentet föreslagit en ny artikel, artikel 13 a, om standardiserade informationsstrategier rörande information som ska lämnas innan information lämnas enligt artikel 14. Informationen enligt artikel 13 a ska vidare lämnas i strukturerad i tabellform och med användning av bildsymboler som parlamentet utformat och som föreslås tas in som en bilaga till uppgiftsskyddsförordningen.

När det gäller artiklarna 14 och 15 har parlamentet föreslagit ett antal tillägg, som dock inte redovisas närmare här. I artikel 21 föreslås att möjligheten att begränsa den registrerades rättigheter enligt punkten c endast ska avse skattefrågor.

Några kommentarer

Som redan konstaterats kommer uppgiftsskyddsförordningens bestämmelser om information till den registrerade att innebära vissa ytterligare skyldigheter jämfört med vad som följer av dataskyddsdirektivet.

När det gäller frågan om information på begäran torde det inte längre vara möjligt att på nationell nivå kräva en skriftlig och egenhändigt undertecknad begäran från den registrerade eller fastställa att rätten endast gäller en gång per år.

I övrigt bedömer vi att varken de nya kraven vad gäller vilken information som ska ges, självmant eller på begäran, eller förfarandekraven kommer att innebära några egentliga problem för myndigheterna. Det sagda gäller även den föreslagna skyldigheten att i vissa fall tillhandahålla information i elektronisk form (artikel 15.2). En osäkerhetsfaktor är emellertid den möjlighet som kommissionens föreslås få att fastställa standardformulär och meddela närmare specificerade krav eller förfaranden i vissa avseenden. Det förefaller dock tveksamt såväl om kommissionen kommer att få dessa möjligheter som, i förekommande fall, om sådana ytterligare bestämmelser kommer att omfatta myndigheters verksamheter.

Av särskild betydelse för myndigheters verksamhet är att undantaget från plikten att självmant ge information rörande personupp-

gifter som inte samlats in från den registrerade när registrering och utlämnande är författningsreglerat föreslås finnas kvar.

13.2 Reglering i registerförfattningar

Information som ska lämnas självmant

Flertalet registerförfattningar saknar särbestämmelser om vilken information som den personuppgiftsansvarige självmant ska lämna till den registrerade i samband med att personuppgifter samlas in från denne.

Handlar det om personuppgifter som samlas in från den registrerade, beror det således på omständigheterna i vad mån och i så fall hur särskild information måste ges eller om förhållandena är sådana att den registrerade redan i sin helhet eller delvis får anses känna till det som informationskravet omfattar (25 § andra stycket PuL).

Det förekommer dock registerförfattningar som ställer krav på att information ska ges i vidare mån än vad som följer av 23 och 25 §§ PuL, detta gäller i synnerhet på områden med anknytning till hälso- och sjukvården. Ett sådant exempel är 13 § apoteksdatalagen (2009:367) enligt vilken den registrerade ska få information, utöver vad som anges i 25 §, om den uppgiftsskyldighet som kan följa av lag eller förordning, de tystnadsplikts- och säkerhetsbestämmelser som gäller för uppgifterna och behandlingen, rätten till skadestånd vid behandling av personuppgifter i strid med lagen, vad som gäller i fråga om sökbegrepp samt vad som gäller i fråga om bevarande.

I de registerförfattningar som ersätter personuppgiftslagen men räknar upp vilka bestämmelser i personuppgiftslagen som ska tillämpas även vid behandling enligt registerförfattningen i fråga, brukar regelmässigt hänvisas till att 23 och 25 §§ PuL ska tillämpas.

Någon motsvarande hänvisning till 24 § PuL, om vilken information som ska ges när personuppgifter samlas in från en annan källa än den registrerade själv, förekommer emellertid normalt sett inte. Det beror på att de särskilda registerförfattningarna i sig eller i förening med annan reglering som styr myndighetens informationshantering anses innehålla tillräckligt preciserade bestämmelser för att utgöra sådana bestämmelser om ”registrerandet eller utlämnandet av personuppgifterna i en lag eller någon annan författning”

som omfattas av undantaget från informationsskyldigheten enligt 24 § andra stycket PuL.

Information som ska lämnas efter ansökan

Inte heller när det gäller rätten att få information efter ansökan enligt 26 § PuL hör det till vanligheterna att registerförfattningarna har bestämmelser som avviker från vad som följer av personuppgiftslagen. Det normala är alltså att registrerade vid behandling av personuppgifter enligt en registerförfattning kan åberopa 26 § PuL till stöd för en ansökan om information och få motsvarande information som om behandlingen enbart reglerats av personuppgiftslagen.

Det förekommer emellertid viss särreglering. Exempelvis finns det bestämmelser som gör skillnad mellan uppgifter som förekommer i handlingar och andra uppgifter när det gäller vad som ska tas med i information enligt 26 § PuL. Enligt 114 kap. 30 § SFB behöver personuppgifter i handlingar som kommit in i ett ärende eller upprättats i ett ärende inte tas med i information enligt 26 § PuL, om den registrerade tagit del av handlingens innehåll. Av informationen ska det däremot framgå vilka sådana handlingar som behandlas. Om den registrerade begär information om uppgifter i en sådan handling och anger vilken handling som avses, ska informationen dock omfatta dessa uppgifter om inte annat följer av bestämmelser om sekretess. I så fall ska begränsningen i 26 § PuL om att information bara behöver lämnas gratis en gång per kalenderår gälla varje handling för sig.

Likartade bestämmelser finns i flera andra registerförfattningar, t.ex. i de som gäller för Skatteverkets beskattningsverksamhet och för Kronofogdemyndigheten. I förarbetena till dessa båda lagar gjorde regeringen följande uttalande avseende dels begränsningen i fråga om en registrerad parts rätt att få information om handlingar, dels frågan om en i en handling omnämnd men utomstående persons rätt till information enligt 26 § PuL beträffande innehållet i handlingen (prop. 2000/01:33 s. 106 f.). I citatet åsyftade sökbegränsningar avser bestämmelser i de aktuella lagarna om att bara vissa uppgifter får användas vid sökning efter elektroniska handlingar i databaser som regleras i lagarna.

> Den enskilde har i detalj kännedom om uppgifterna i handlingarna sedan tidigare, eftersom dessa antingen har getts in av eller expedierats till honom med det registrerade innehållet. Att en myndighet då i information till en registrerad tydligt anger vilka elektroniska handlingar som behandlas i en databas eller i ett ärende som rör denne torde enligt regeringens mening vara tillräckligt för att uppfylla dataskyddsdirektivets krav på att de registrerade i detalj skall kunna kontrollera om uppgifterna är korrekta eller inte. Regeringen anser därför i likhet med utredningen att elektroniska handlingar inte behöver lämnas ut till en enskild i samband med att en personuppgiftsansvarig myndighet fullgör sin informationsskyldighet enligt 26 § personuppgiftslagen, om den enskilde har tagit del av handlingens innehåll. Enskilda bör emellertid inte helt fråntas rätten att med tillämpning av 26 § personuppgiftslagen ta del av elektroniska handlingar som de har gett in eller som har expedierats till dem. Fullständig information om vilka uppgifter som behandlas, således även uppgifter i elektroniska handlingar, bör enligt regeringens mening lämnas om den enskilde begär det.
>
> En annan fråga är vad som skall gälla i fråga om personer som finns omnämnda i handlingar som hör till ett ärende i vilket de inte själva är part. Dessa personer omfattas inte av det föreslagna undantaget eftersom de med största sannolikhet inte fått del av handlingarna. Det innebär emellertid enligt regeringens mening inte att de har rätt att enligt 26 § personuppgiftslagen få information om behandlingen. Regeringen har tidigare i den proposition som låg till grund för personuppgiftslagen (prop. 1997/98:44, s. 83) uttalat bl.a. att det är rimligt att utgå från att Datalagskommitténs slutsats att EG-direktivet innebär att den personuppgiftsansvarige bara är skyldig att utnyttja alla de sök- och sammanställningsmöjligheter som han har tillgång till för att få fram information att lämna den registrerade är riktig. Regeringens förslag om sökbegränsningar […] innebär att myndigheterna saknar rättsliga befogenheter, och vanligen även tekniska möjligheter, att kontrollera i vilken omfattning uppgifter om en person behandlas i handlingar som hör till ett ärende som inte rör honom. Därmed har enligt regeringens mening en person som är registrerad på ett sådant sätt inte heller rätt att kräva att myndigheten gör den typen av kontroller.

Enligt 13 § lagen (2012:741) om behandling av personuppgifter vid Institutet för arbetsmarknads- och utbildningspolitisk utvärdering gäller inte 26 § PuL i fråga om personuppgifter som inte direkt kan hänföras till en person. I 18 § lagen (2001:99) om den officiella statistiken anges på liknande sätt att den som har fått kodade personuppgifter från en statistikansvarig myndighet inte behöver lämna information till den registrerade om att uppgifter behandlas, om

den som behandlar uppgifterna inte själv har möjlighet att vidta någon åtgärd för att identifiera den registrerade.

Ett undantag i annan slags reglering än registerförfattning är 7 a § arkivförordningen (1991:446). Där föreskrivs att en arkivmyndighet inte behöver lämna besked och information enligt 26 § PuL när det gäller personuppgifter i arkivmaterial som tagits emot för förvaring av myndigheten, om detta visar sig vara omöjligt eller skulle innebära en oproportionerligt stor arbetsinsats. Motsvarande bestämmelse fanns tidigare i 10 § datalagen.

13.3 Andra bestämmelser om rätt till information på begäran

Som vi redan har berört finns vid sidan av de bestämmelser om information som följer av 23–26 §§ PuL alternativa sätt för registrerade att få insyn i myndigheters behandling av personuppgifter om honom eller henne.

Under ett pågående förfarande som berör en registrerad, t.ex. en sökande i ett ärende, har denne ofta en långtgående rätt till insyn i ärendet och myndigheten har en skyldighet att se till att sökanden får del av information som tillförts ärendet av annan än sökanden själv. Sådana bestämmelser om partsinsyn och kommunikationsplikt är dock främst av betydelse under pågående förfaranden och ger inte annan än part eller motsvarande rätt till information.

Var och en har emellertid rätt att med stöd av 2 kap. TF få del av myndigheters allmänna handlingar. Den rätten kan bara begränsas på grund av sekretess.

Sekretess för en personuppgift till skydd för enskilds intresse gäller oftast inte i förhållande till den person som uppgiften avser, se 12 kap. 1 § OSL. Däremot kan sekretess till skydd för allmänna intressen eller till skydd för annan enskilds intressen hindra insyn. Det sistnämnda kan t.ex. vara fallet när uppgifter samtidigt berör flera personer och har lämnats av någon annan person vars intresse av att uppgifterna inte röjs för de övriga personerna skyddas av en sekretessbestämmelse.

Avgörande för rätten till insyn enligt 2 kap. TF är att handlingen blivit allmän genom att antingen ha kommit in till eller ha upprättats hos myndigheten. När det gäller handlingar som behandlas

med modern informationsteknik är rätten till insyn mycket vidsträckt i och med att den enskilde kan begära att myndigheten gör sammanställningar av uppgifter ur upptagningar, s.k. potentiella handlingar. Sådan information som avses i 26 § PuL kan många gånger motsvara en sammanställning av uppgifter som i 2 kap. TF:s mening utgör en potentiell handling, i vart fall såvitt avser myndighetens redovisning av vilka personuppgifter som behandlas.

Rätten att begära ut potentiella handlingar begränsas bara, förutom av sekretess, av att myndigheten måste kunna göra sammanställningen dels med rutinbetonade åtgärder, dels utan att bryta mot något sökförbud eller liknande i lag eller förordning som gäller för myndigheten. Går sammanställningen inte att ta fram med rutinbetonade åtgärder eller utan att bryta mot någon ovillkorlig sökbegränsning i lag eller förordning är den potentiella handlingen inte allmän (2 kap. 3 § TF).

En sökande som vill få insyn i allmänna handlingar måste kunna precisera sin begäran, dvs. kunna med viss tydlighet ange vilken eller vilka handlingar som han eller hon vill ta del av. En myndighet är nämligen inte skyldig att bedriva mer omfattande efterforskning, huruvida vissa handlingar i arkiverat material omfattas av en allmänt hållen beskrivning (RÅ79 Ab 6). Vid en begäran hos en myndighet att få ta del av alla beslut rörande en viss namngiven person, utan begränsning till slag eller tid, torde en myndighet inte behöva göra mer än att använda tillgängliga register för att göra sökningar (jfr NJA 1998 a. 559).

Rätten att ta del av allmänna handlingar omfattar inte bara att på plats hos myndigheten få läsa handlingar (2 kap. 12 § TF). Var och en har också rätt att mot en avgift få kopior av allmänna handlingar. Det gäller oavsett om det är fråga om en traditionell handling på papper eller om det är en handling i form av en upptagning som behandlas elektroniskt. Det finns dock, som huvudregel, ingen rätt att få elektroniska kopior. Den rätt som följer av tryckfrihetsförordningen är att få en pappersutskrift (2 kap. 13 §). Kostnaden för detta regleras närmare i avgiftsförordningen (1992:191). Någon motsvarande rätt att gratis få skriftlig information som följer av 26 § PuL finns således inte. Å andra sidan gäller betydligt mer strikta krav på skyndsamhet vid utfående av kopior enligt tryckfrihetsförordningen än vad som är fallet med information enligt 26 § PuL.

Utöver skyldigheten att på begäran lämna ut allmänna handlingar är myndigheter också skyldiga att på begäran av en enskild lämna uppgifter ur myndighetens allmänna handlingar. Detta följer av 6 kap. 4 § OSL. Skyldigheten kan bara begränsas på grund av sekretess eller om det skulle hindra arbetets behöriga gång att lämna ut uppgifterna.

13.4 Våra överväganden och förslag

13.4.1 Information som ska lämnas självmant

Förslag och bedömning: Personuppgiftslagens bestämmelser om information som självmant ska lämnas till den registrerade ska gälla vid myndigheters behandling av personuppgifter enligt den nya lagen. Det ska framgå genom en hänvisning till 23 och 25 §§ PuL. Det behövs inte någon bestämmelse om att information ska ges då uppgifter samlas in från någon annan källa än den registrerade. Någon hänvisning till 24 § PuL bör därför inte göras.

Information när personuppgifter samlas in från den registrerade

De bestämmelser som finns i 23 och 25 §§ PuL angående information som ska ges till den registrerade när uppgifter samlas in från personen själv är i sak desamma som följer av artikel 10 i direktivet. Såvitt vi erfarit medför dessa bestämmelser inga särskilda tillämpningsproblem för myndigheterna. Det har inte heller framkommit att det generellt sett skulle behövas mer information än vad som anges i 25 § första stycket för att tillgodose de registrerades behov. Det är därför vår uppfattning att den nya lagen inte bör innehålla bestämmelser som avviker från 23 och 25 §§ PuL när det gäller information som ska lämnas då personuppgifter samlas in från den registrerade.

Det sagda gäller även bestämmelsen i 25 § andra stycket PuL om att information inte behöver lämnas om sådant som den registrerade redan känner till. Det undantaget har stor betydelse för myndigheter och sådana slag av behandlingar då den enskilde regelmässigt kan förutsättas vara införstådd med personuppgiftsbehandlingen

även utan att ha fått någon särskild information. Det kan gälla så självklara situationer som när en enskild kontaktar en myndighet via e-post. Det ligger då i sakens natur att detta innebär behandling av personuppgifter och att denna behandling kan antas komma att föranleda en viss ytterligare personuppgiftsbehandling hos myndigheten. Detsamma gäller t.ex. sådan ärendehandläggning som föranleds av en sökandes ansökan om något, t.ex. ett visst tillstånd. I dessa fall torde det vara fullt tillräckligt att myndigheten håller tillgänglig en sådan allmänt inriktad information med förteckning över myndighetens personuppgiftsbehandlingar m.m. som vänder sig till både allmänhet och en allmän krets av registrerade. Vi återkommer till detta i avsnitt 16.4.

I andra fall – t.ex. i samband med att enskilda som en serviceåtgärd erbjuds att ansluta sig till en e-tjänst för inrapportering av uppgifter till en myndighet – bör det däremot åligga en personuppgiftsansvarig myndighet att se till att den enskilde nås av adekvat information. Ingen bör t.ex. kunna få ansluta sig till en e-tjänst som inbegriper personuppgiftsbehandling utan att ha fått tillräcklig information om vilken personuppgiftsbehandling som äger rum i samband med just den e-tjänsten.

Såvitt vi kan se möjliggör 23 och 25 §§ PuL den flexibilitet som måste finnas i en reglering av nu aktuellt slag. Mot denna bakgrund menar vi alltså att bestämmelserna i 23 och 25 §§ PuL bör vara tillämpliga även vid myndigheters behandling av personuppgifter enligt den nya lagen. Detta bör framgå genom en hänvisning till att dessa bestämmelser ska vara tillämpliga även vid behandling enligt lagen.

Vi har i avsnitt 8.3 gjort bedömningen att myndigheters personuppgiftsbehandling enligt vår uppfattning inte i något fall bör stödjas på missbruksregeln i 5 a § PuL och vi har föreslagit att den bestämmelsen inte ska vara tillämplig vid behandling av personuppgifter enligt den nya lagen. Vi har därför ställt oss frågan om det behövs något undantag från informationsskyldigheten enligt 23 och 25 §§ som i något avseende motsvarar den lättnad som torde följa av missbruksregeln. Vi ser emellertid inte att det finns något sådant behov i fråga om information som ska lämnas i samband med att uppgifter samlas in från den registrerade.

Information när personuppgifter samlas in från annan källa än den registrerade

Vi har vad gäller information som ska lämnas om personuppgifter har samlats in från någon annan källa än den registrerade (24 § första stycket PuL) inte heller nåtts av signaler om att paragrafen inte skulle vara ändamålsenligt utformad eller medföra några särskilda problem för myndigheterna. Det framstår dock som oklart i vad mån det finns myndigheter som anser sig omfattas av den bestämmelsen. Enligt 24 § andra stycket behöver information enligt första stycket nämligen inte ges om det finns bestämmelser om ”registrerandet eller utlämnandet av personuppgifterna” i lag eller annan författning. Enligt artikel 11.2 i direktivet ska det vara fråga om uttryckliga föreskrifter. Det är dock inte närmare beskrivet vilken grad av precision som krävs för att bestämmelser ska anses vara sådana uttryckliga föreskrifter som medför att information inte behöver lämnas.

Frågan måste därför ställas om bestämmelserna i den nu föreslagna lagen utgör sådana föreskrifter. Om så inte är fallet uppkommer frågan om det finns andra kompletterande bestämmelser som styr myndigheternas verksamheter och därmed informationshantering och som i stället för eller tillsammans med den nya lagen kan anses utgöra sådana föreskrifter som innebär ett undantag från informationsskyldigheten.

Bestämmelserna i registerförfattningar har ofta ansetts vara av det slag som avses i 24 § andra stycket PuL. Att det förhåller sig på det viset kan knappast ifrågasättas när det handlar om den typ av renodlade registerförfattningar som föreskriver att ett visst register av visst innehåll ska föras. Mer tveksamt kan det måhända te sig beträffande det vi kallar informationshanteringsförfattningar som alltså anger vad myndigheterna får göra i form av personuppgiftsbehandling. De informationshanteringsförfattningar som utformats utifrån modellen att hänvisa till vilka bestämmelser i personuppgiftslagen som ska vara tillämpliga även vid behandling enligt lagen i fråga hänvisar emellertid inte till 24 § PuL. Skälet torde vara att det ansetts att sådana lagar – som gäller för bl.a. Skatteverkets beskattnings- och folkbokföringsverksamhet, Kronofogdemyndigheten, Tullverkets tullverksamhet, Polisens brottsbekämpande verksamhet och Kustbevakningen – är specialutformade för verksam-

heterna i fråga. De innehåller preciserade regler som sedda tillsammans med den verksamhetsreglering som i övrigt gäller för myndigheterna i fråga kan ses som sådana uttryckliga bestämmelser om registrering eller utlämnande som krävs enligt artikel 11.2 i direktivet.

Den nu föreslagna lagen kommer att tillämpas av ett mycket stort antal myndigheter. De bestämmelser som vi föreslår är följaktligen generellt utformade. Det kan tyckas att lagen som sådan därför inte lever upp till kravet på att vara en uttrycklig reglering om ”registrerande eller utlämnande” av personuppgifter. Samtidigt ska beaktas att sådana särregler som kommer att behöva meddelas i anslutning till lagen tveklöst torde utgöra bestämmelser av det slag som avses i 24 § andra stycket och som medför undantag från informationsskyldigheten. Så kan t.ex. vara fallet beträffande regler som syftar till att möjliggöra direktåtkomst avseende sekretessreglerade personuppgifter m.m. I avsaknad av sådana särskilda regler uppkommer frågan i vilken mån den övriga reglering som gäller för myndigheternas verksamheter har betydelse i sammanhanget.

Det kan då konstateras att det är ett grundläggande förhållande att all förvaltningsverksamhet på det ena eller andra sättet är författningsstyrd. Detta gäller även i fråga om myndigheternas informationshantering. Utgångspunkten är vidare att myndigheter inte samlar in personuppgifter om enskilda från annan än den registrerade själv utan att detta sker med författningsstöd som – i vart fall indirekt – ålägger eller tillåter myndigheter att samla in och registrera uppgifter av det slaget. På samma sätt förhåller det sig med utlämnande av personuppgifter. Det ska i princip inte förekomma utlämnanden som inte har i vart fall indirekt stöd i författningsreglering. Mot denna bakgrund anser vi att den samlade författningsregleringen av myndigheternas verksamheter och därmed informationshantering i kombination med den föreslagna lagen om myndigheters behandling av personuppgifter är tillräcklig för att uppfylla kraven enligt direktivet i detta hänseende. Det finns, som vi ser det, därför inga skäl att ålägga myndigheter att självmant lämna ytterligare information till registrerade rörande sådana förhållanden som avses i 24 § första stycket PuL.

Sammanfattningsvis gör vi således bedömningen att det inte behövs någon hänvisning till 24 § PuL eftersom det alltid kan antas

finnas bestämmelser om myndigheters registrerande och utlämnande av personuppgifter i författning.

13.4.2 Information som ska lämnas efter ansökan

Förslag: Personuppgiftslagens bestämmelse om den registrerades rätt att efter ansökan få information ska gälla även vid myndigheters behandling av personuppgifter enligt den nya lagen. Det ska framgå genom en hänvisning till 26 § PuL. Rätten till information efter ansökan ska dock bara gälla i fråga om personuppgifter som ingår i eller är avsedda att ingå i en samling av personuppgifter som har strukturerats för att påtagligt underlätta sökning efter eller sammanställning av personuppgifter. Ett särskilt undantag görs därmed för uppgifter i s.k. ostrukturerat material, vilket motsvarar vad som i dag följer av den s.k. missbruksregeln i 5 a § PuL.

Som vi berört tidigare gjordes vid personuppgiftslagens tillkomst ingen närmare analys av vad direktivets krav innebar på myndighetsområdet, t.ex. i vad mån det redan fanns reglering av förvaltningsrättslig natur m.m. som i sak förverkligade direktivets krav.

En fråga som enligt vår mening möjligen kunde ha ställts var om det verkligen var till alla delar motiverat att genomföra 12 a i direktivet om den registrerades rätt till tillgång till uppgifter på så sätt att regleringen i 10 § datalagen om registerutdrag arbetades in i personuppgiftslagen men med ett betydligt mera vidsträckt tillämpningsområde än vad som hade varit fallet under datalagens tid. Då handlade det om en rätt att få regelrätta utdrag ur automatiserade personregister. Med personuppgiftslagen kom rätten till ”utdrag” att omfatta alla personuppgifter som behandlas helt eller delvis automatiserat eller i manuella register alldeles oavsett om behandlingen sker i eller i anslutning till något register, ärendehanteringssystem eller annan strukturerad informationssamling.

Till saken hör att den registrerade har helt andra möjligheter än i enskild verksamhet att med stöd av offentlighetsprincipen få insyn i den personuppgiftsbehandling som sker i den offentliga verksamheten. Den registrerade har alltså en rätt till insyn i allmänna handlingar och kan åberopa 2 kap. TF för att få del av allmänna hand-

lingar med personuppgifter som rör den registrerade själv. På så sätt kan han eller hon kontrollera personuppgifterna i deras rätta sammanhang, vilket inte sällan torde ge bättre förutsättningar att tillgodogöra sig innebörden av och bedöma lagenligheten i personuppgiftsbehandlingen i fråga än vad ett utdrag med sammanställda personuppgifter ger. I sammanhanget kan erinras om att syftet med direktivets bestämmelse om den registrerades rätt till tillgång till uppgifterna är att denne i detalj ska kunna försäkra sig om att uppgifterna är korrekta och om att behandlingen är tillåten (punkt 41 i ingressen till direktivet), ett syfte som den registrerades rätt till insyn i allmänna handlingar väl tillgodoser. Rätten till insyn enligt offentlighetsprincipen kan vidare utnyttjas i princip hur ofta som helst – och formlöst – medan rätten enligt 26 § PuL bara kan utövas en gång om året och då efter skriftlig ansökan.

Samtidigt finns det andra skillnader mellan rätten till insyn enligt 26 § PuL och 2 kap. TF. Rätten enligt personuppgiftslagen ger t.ex. i princip en möjlighet till insyn i handlingar som inte är allmänna samt ytterligare upplysningar om mottagare eller mottagarkategorier. Av väsentlig betydelse är också kravet på information om ändamålen med behandlingen.

Man hade emellertid möjligen kunnat tänka sig att det hade räckt för att uppfylla direktivets krav att vid genomförandet, såvitt avser myndigheter, hänvisa till den registrerades rätt att få tillgång till allmänna handlingar eller uppgifter ur allmänna handlingar. Den sammantagna effekten av handlingsoffentligheten, myndigheternas skyldighet att anmäla eller upplysa allmänheten om ändamål, mottagarkategorier m.m. (artiklarna 19 och 21, jfr 36 och 42 §§ PuL) och en allmän hänvisning till myndigheternas serviceskyldighet skulle måhända ha kunnat anses motsvara direktivets krav. Artikel 12 a i direktivet ställer nämligen inte krav på att medlemsstaterna ska införa särskilda föreskrifter. Det som krävs är att medlemsstaterna ska säkerställa rätten till information och insyn, vilket torde lämna viss frihet för medlemsstaterna att välja metod för hur denna rätt ska förverkligas. Enligt vår uppfattning finns i och för sig inget hinder mot att vid sådant förhållande anse att redan existerande inhemska författningsreglerade rättigheter tillgodoser direktivets krav, så länge som dessa i praktiken leder till det resultat som ska uppnås.

Vi ser dock ingen anledning att nu föreslå några förändringar vad gäller frågan om hur artikel 12 a i direktivet har genomförts på myndighetsområdet. Som anfördes i förarbetena till 2006 års ändringar av personuppgiftslagen fyller rätten att på begäran få ett ”registerutdrag” en viktig kontrollfunktion, särskilt när det gäller uppgifter i regelrätta register eller stora databaser. Av väsentlig betydelse är vidare, som vi ser det, att informationsskyldigheten enligt 26 § PuL också innefattar en redovisning av ändamålen med behandlingen. I den mån dessa inte är författningsreglerade innebär detta en viktig kontrollfunktion för enskilda registrerade. Mot den bakgrunden skulle det kunna sägas innebära en klar försämring av enskildas rättsskydd om rätten till information på begäran togs bort. Även enligt den nya lagen bör myndigheter således ha en skyldighet att på begäran lämna sådan information som avses i 26 § PuL. Vi föreslår att detta ska framgå genom en hänvisning till den paragrafen.

Eftersom vi alltså är av uppfattningen att missbruksregeln inte ska gälla enligt den nya lagen inställer sig även här frågan om ett särskilt undantag behöver göras beträffande personuppgifter som förekommer i sådana sammanhang.

De överväganden som föranledde att missbruksregeln kom att även omfatta skyldigheten att lämna s.k. registerutdrag enligt 26 § PuL har, menar vi, bärighet också på myndigheternas område. Att nuvarande registerlagar inte har motsvarande begränsningar i sina hänvisningar till 26 § PuL torde bero på att dessa lagar i allt väsentligt reglerar antingen personuppgifter som strukturerats för att påtagligt underlätta sökning efter eller sammanställning av personuppgifter (personregister) eller personuppgifter som ingår i eller är avsedda att ingå i strukturerade informationssamlingar (t.ex. personuppgifter i ärendehanteringsystem eller i färdiga elektroniska handlingar som är kopplade till ett ärendehanteringssystem).

Den nya lagen kommer att tillämpas av såväl små som stora myndigheter, oavsett vad för slags personuppgiftsbehandlingar som avses och oavsett om eller i vilken utsträckning en myndighet förfogar över material med personuppgiftsanknuten struktur. Det är rimligt, menar vi, att myndigheter som grundregel även i fortsättningen har en lättad informationsplikt såvitt avser ”registerutdragen” motsvarande den som följer av nuvarande 5 a § första stycket PuL. Vi föreslår därför en sådan regel.

Enligt vår mening är ett fortsatt undantag avseende information om personuppgifter i ostrukturerat material förenlig med direktivet. Det framgår redan av det ovan sagda om att handlingsoffentligheten och rätten att få uppgifter ur allmänna handlingar tillsammans med myndigheters övriga serviceskyldigheter kan anses i princip säkerställa den registrerades rätt till tillgång enligt artikel 12 a i direktivet. Till det kommer våra förslag i avsnitt 16.4 om att varje myndighet ska föra en förteckning över de behandlingar som utförs med stöd av den nya lagen.

Förslaget innebär alltså ingen saklig ändring i förhållande till dagens reglering. Genom att personuppgifter i s.k. ostrukturerat material även fortsättningsvis undantas från informationsskyldigheten klargörs att myndigheter t.ex. inte behöver söka igenom alla befattningshavares e-post eller hårddiskar m.m. Ledning beträffande gränsdragningen mellan personuppgifter som ingår i respektive inte ingår i en samling av personuppgifter som har strukturerats för att underlätta sökning efter eller sammanställning av personuppgifter finns i förarbetena till 5 a § PuL. Där anges bl.a. att behandling av personuppgifter t.ex. i löpande text i ordbehandlingsprogram, e-postmeddelanden, på internet eller enstaka ljud- och bildupptagningar faller inom det undantagna området. Om uppgifterna i den löpande texten, i ljud- och bildupptagningen osv. däremot infogas i en databas med en personuppgiftsanknuten struktur, exempelvis ett ärendehanteringssystem, är behandlingen inte undantagen från personuppgiftslagens hanteringsregler (prop. 2005/06:173 s. 19–25 och 58). Se även Högsta förvaltningsdomstolens domar den 8 januari 2014 i mål nr 571-14 och 642-14.

13.4.3 Begränsningar i informationsplikten på grund av sekretess

Förslag: Sekretess ska på samma sätt som enligt personuppgiftslagen begränsa informationsskyldigheten enligt den nya lagen. Det ska framgå av en bestämmelse som motsvarar 27 § PuL.

På motsvarande sätt som gäller enligt personuppgiftslagen bör sekretess för uppgifter som gäller gentemot den registrerade inskränka myndigheternas informationsskyldighet. I förtydligande syfte bör

någon hänvisning emellertid inte göras till den bestämmelse i personuppgiftslagen (27 §) av vilket detta kan utläsas. I den nya lagen bör i stället införas en ny bestämmelse som klargör att det i detta hänseende bara är sekretess enligt offentlighets- och sekretesslagen eller föreskrifter som meddelats med stöd av den lagen som kan inskränka informationsskyldigheten.

14 Bevarande och gallring

14.1 Arkivlagstiftningen

Handlingsoffentligheten och elektronisk informationshantering

Enligt 2 kap. 1 § TF har varje svensk medborgare en grundlagsfäst rätt att ta del av myndigheters och andra offentliga organs allmänna handlingar. Av bestämmelsen framgår att syftet härmed är att främja ett fritt meningsutbyte och en allsidig upplysning. Rätten att ta del av allmänna handlingar är ett av de viktigaste inslagen i offentlighetsprincipen, dvs. den grundsats som innebär att samhällsorganens verksamhet ska bedrivas under allmän insyn och kontroll. Handlingsoffentlighetens syften brukar, utöver vad som anges i 2 kap. 1 § TF, sammanfattningsvis sägas vara att garantera rättssäkerheten samt effektiviteten i förvaltningen och i folkstyret.

Vad som är en allmän handling definieras i 2 kap. TF. Vi har relativt ingående redogjort för dessa bestämmelser i vårt delbetänkande med fokus på innebörden av regleringen i fråga om elektroniskt lagrad information, se SOU 2012:90 s. 60 f. samt 91 f. I den elektroniska miljön brukar man tala om två handlingsslag, dels färdiga elektroniska handlingar, dels sammanställningar av uppgifter, s.k. potentiella handlingar. Utmärkande för det sistnämnda handlingsslaget är att varje tänkbar sammanställning av uppgifter ur en eller flera upptagningar kan vara en allmän handling alldeles oavsett om den vid ett givet tillfälle har eller inte har existerat tidigare i sammanställd form. För sammanställningar av uppgifter gäller dock enligt 2 kap. 3 § TF särskilda undantag från vad som konstituerar allmänna handlingar.

För att offentlighetsprincipen i form av handlingsoffentlighet ska få genomslag och kunna utnyttjas i praktiken krävs inte bara en god offentlighetsstruktur m.m. (se 4 och 5 kap. OSL). Det krävs också att allmänna handlingar bevaras även efter det att deras omedel-

bara nytta i den löpande verksamheten har upphört. Myndigheterna har därför grundläggande skyldigheter att bevara sina allmänna handlingar i arkiv.

Arkivvård och gallring

En myndighets allmänna handlingar ska hållas ordnade och vårdas bl.a. för att tillgodose allmänhetens rätt att ta del av allmänna handlingar i ett långsiktigt perspektiv.

Arkivsystemets anknytning till handlingsoffentligheten tydliggjordes i samband med 2001 års ändringar av 2 kap. TF genom införandet av 2 kap. 18 § TF. Den bestämmelsen syftar till att betona arkivreglernas betydelse för offentlighetsinsynen enligt 2 kap. TF och innebär att grundläggande bestämmelser om hur allmänna handlingar ska bevaras samt om gallring och annat avhändande enbart kan meddelas genom lag (prop. 2001/02:70 s. 39).

Varje myndighet är ansvarig för arkivvården av den egna myndighetens handlingar. I arkivvården ingår emellertid även att se till att arkiven inte kommer att omfatta onödigt material och att handlingarna efterhand gallras (prop. 1989/90:72 s. 38).

Grundläggande bestämmelser om bevarande och gallring av allmänna handlingar hos statliga och kommunala myndigheter finns i arkivlagen (1990:782). Lagen är en ramlag som innehåller allmänna och övergripande bestämmelser om myndigheternas arkiv. Flertalet bestämmelser är teknikoberoende och avser såväl pappershandlingar som elektroniskt lagrade upptagningar. Lagen fylls ut av arkivförordningen (1991:446) samt de myndighetsspecifika beslut eller generella föreskrifter som arkivmyndigheterna utfärdar. Riksarkivet är statlig arkivmyndighet. Kommunstyrelsen är arkivmyndighet i en kommun och landstingsstyrelsen i ett landsting, om inte kommunfullmäktige eller landstingsfullmäktige har utsett någon annan nämnd eller styrelse till arkivmyndighet. Arkivmyndigheter kan med tiden överta arkivmateriel från myndigheter som står under deras tillsyn.

I 3 § arkivlagen slås fast att myndigheternas arkiv är en del av det nationella kulturarvet och att de ska bevaras, hållas ordnade och vårdas så att de tillgodoser

1. rätten att ta del av allmänna handlingar,
2. behovet av information för rättskipningen och förvaltningen, och
3. forskningens behov.

En myndighets arkiv bildas av de allmänna handlingarna från myndigheternas verksamhet. Så snart ett ärende slutbehandlats ska de allmänna handlingarna arkiveras och myndigheten ska pröva i vilken omfattning minnesanteckningar, utkast eller liknande handlingar som avses i 2 kap. 9 § TF ska rensas bort eller tas om hand för arkivering, vilket innebär att de blir allmänna handlingar. Allmänna handlingar som inte tillhör ett ärende ska arkiveras så snart de justerats av myndigheten eller på annat sätt färdigställts. I diarier och journaler eller register och förteckningar som förs fortlöpande ska varje införd anteckning anses arkiverad i och med den har gjorts (3 § arkivförordningen).

Arkivering är ett teknikneutralt begrepp. Elektronisk arkivering av allmänna handlingar är alltså fullt möjligt och är på stark framväxt i den offentliga förvaltningen. För närvarande pågår flera myndighetsövergripande projekt rörande digital arkivering i s.k. e-arkiv. Riksarkivet har lett ett projekt eARD som tagit fram förvaltningsgemensamma specifikationer (FGS:er) för e-arkiv och e-diarium. Även Sveriges Kommuner och Landsting driver projekt om e-arkiv hos kommuner och landsting.

Huvudprincipen enligt arkivlagen är att allmänna handlingar ska bevaras i myndigheternas arkiv. Denna huvudprincip gäller dock inte utan undantag.

För elektronisk information gäller till en början ett undantag vid situationer då flera myndigheter har tillgång till samma upptagning. Om en upptagning för automatiserad behandling är tillgänglig för flera myndigheter så att den utgör en allmän handling hos alla dessa myndigheter, ska upptagningen bilda arkiv endast hos en av myndigheterna, i första hand den myndighet som svarar för huvuddelen av upptagningen (3 § arkivlagen). Svarar statliga myndigheter för ungefär lika stora delar av upptagningen, får Riksarkivet meddela föreskrifter om hos vilken myndighet upptagningen ska bilda arkiv (4 § arkivförordningen).

Ett annat undantag från huvudregeln om bevarande är att allmänna handlingar enligt 10 § arkivlagen får gallras. Därvid ska alltid beaktas att arkiven utgör en del av kulturarvet och att det arkivmaterial som återstår ska kunna tillgodose rätten att ta del av allmänna handlingar, behovet av information för rättskipningen och förvaltningen samt forskningens behov. Med forskning avses i arkivlagen inte enbart professionell, vetenskaplig forskning utan även amatörforskning, t.ex. släktforskning.

Det kan således konstateras att arkivlagen inte föreskriver att bevarande- och gallringsfrågor ska beaktas också utifrån hänsynstagande till intresset av skydd för den personliga integriteten. Gallring i arkivhänseende sker närmast av praktiska och ekonomiska skäl och syftar enligt arkivlagens motiv till att arkiven inte ska tyngas av handlingar som saknar påtagligt informationsvärde, som bara utgör dubblering av information som bättre kan sökas i ett annat arkiv eller som har ett informationsvärde som är markant begränsat i tiden. En riktigt utförd gallring bör därmed leda till att arkiven blir mer överskådliga och effektiva som informationskällor (prop. 1989/90:72 s. 40 f.).

Gallring av traditionella pappershandlingar innebär att dessa förstörs fysiskt. När det gäller gallring av elektroniska upptagningar avses normalt att viss information raderas från databäraren. Det är dock inte nödvändigt att den egentliga information som finns på ett elektroniskt medium verkligen förstörs för att det ska vara fråga om gallring. Gallring kan exempelvis också ske genom att elektroniskt lagrad information skrivs ut på papper varefter den elektroniska versionen raderas. Ett annat exempel kan vara att en excel-fil med en samling uppgifter sparas i ett pdf-dokument som överförs till ett usb-minne, varefter excel-filen raderas från datorn. Även om möjligheten till insyn som sådan inte försvinner vid sådan partiell gallring – informationen finns ju kvar på pappret eller i pdf-dokumentet – så kan förutsättningarna för att söka fram eller sammanställa informationen påtagligt ha försämrats.

Riksarkivet har i 2 kap. 1 § Riksarkivets föreskrifter och allmänna råd om elektroniska handlingar (upptagningar för automatiserad behandling; RA-FS 2009:1) definierat gallring som förstöring av allmänna handlingar eller förstöring av uppgifter i allmänna handlingar. Det är också fråga om gallring när andra åtgärder vidtas med allmänna handlingar som medför förlust av betydelsebärande data,

förlust av möjliga sammanställningar, förlust av sökmöjligheter, eller förlust av möjligheter att bedöma handlingarnas autenticitet.

Begreppsapparaten på arkivområdet innebär att det bara är allmänna handlingar som gallras. Vid förstöring av handlingar som inte är allmänna handlingar talar man om rensning. Då myndigheter sorterar bort minnesanteckningar, utkast, föredragningspromemorior och andra sådana handlingar som avses i 2 kap. 9 § TF i syfte att de inte ska tas om hand för arkivering, sker således en rensning och inte en gallring.

Överföring av allmänna handlingar från ett ursprungligt datamedium till ett datamedium för digital arkivering torde i sig inte innebära gallring i arkivlagens mening så länge några förluster av sökmöjligheter inte uppstår (se t.ex. prop. 2011/12:45 s. 175).

En statlig myndighet får inte på egen hand med tillämpning av 10 § arkivlagen avgöra vilka allmänna handlingar som ska gallras ur dess arkiv. Allmänna handlingar hos myndigheten får endast gallras i enlighet med föreskrifter eller beslut av Riksarkivet, om inte särskilda gallringsföreskrifter finns i lag eller förordning (14 § arkivförordningen). Sådana särskilda gallringsföreskrifter finns ofta i registerförfattningar och gäller i stället för arkivlagens bestämmelser oavsett om de förekommer i lag eller förordning. Detta följer av 10 § tredje stycket arkivlagen enligt vilken arkivlagen är subsidiär till avvikande bestämmelser om gallring av vissa allmänna handlingar i lag eller förordning. På det kommunala området gäller att beslut om gallring kan meddelas av kommunfullmäktige respektive landstingsfullmäktige som då, liksom Riksarkivet, har att följa de yttre ramar för gallring som anges i 10 § arkivlagen. Inte heller på det kommunala området får alltså en arkivbildande myndighet själv avgöra vad som ska gallras eller inte.

14.2 Allmänna dataskyddsrättsliga regler

Dataskyddsdirektivet

Enligt artikel 6.1 e i dataskyddsdirektivet ska medlemsstaterna föreskriva att personuppgifter förvaras på ett sätt som förhindrar identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka uppgifterna samlades in eller för vilka de senare behandlades. Medlemsstaterna ska vidare vidta lämp-

liga skyddsåtgärder för de personuppgifter som lagras under längre perioder för historiska, statistiska eller vetenskapliga ändamål. Det är således underförstått att det ligger i den registrerades intresse att personuppgifter inte lagras utan något konkret syfte.

Personuppgiftslagen

Artikel 6.1 e i direktivet har genomförts i Sverige genom 9 § första stycket i PuL enligt vilken det är ett grundläggande krav att den personuppgiftsansvarige ska se till att personuppgifter inte bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen. Det är alltså ändamålen för en personuppgiftsbehandling som avgör hur länge uppgifterna får bevaras. Ospecificerad lagring av personuppgifter som kan vara ”bra att ha” är inte tillåten. Behövs uppgifterna inte längre för ändamålen ska de förstöras eller avidentifieras (SOU 1997:39 s. 353).

Dock får uppgifterna bevaras även därefter så länge det behövs för historiska, statistiska eller vetenskapliga ändamål (9 § tredje stycket). I det sistnämnda fallet får uppgifterna endast i undantagsfall användas för att vidta någon åtgärd i fråga om den registrerade (9 § fjärde stycket).

Om missbruksregeln i 5 a § PuL är tillämplig behöver bestämmelserna i 9 § inte tillämpas. Det innebär att regeln i 9 § första stycket i om längsta bevarandetid inte gäller vid behandling av personuppgifter som inte ingår i en uppgiftssamling med personuppgiftsanknuten struktur.

För myndigheter gäller enligt 8 § andra stycket PuL särskilda regler om förhållandet till arkivbildning. Enligt 8 § andra stycket första meningen hindrar bestämmelserna i personuppgiftslagen inte att en myndighet arkiverar och bevarar allmänna handlingar eller att arkivmaterial tas om hand av en arkivmyndighet. I motiven till bestämmelsen anfördes att myndigheters arkivering kan hänföras till vad direktivet avser med ”historiskt, statistiskt eller vetenskapligt ändamål” varför arkivering inte behöver anges som ett uttryckligt ändamål när personuppgifter samlas in. Är en myndighets primära hantering av uppgifterna tillåten, kan det inte anses oförenligt med den primära hanteringen att bevara uppgifterna. Inte heller kan det anses oförenligt med de ursprungligen angivna ändamålen att myn-

digheten efter en tid lämnar över sina handlingar till en arkivmyndighet för långtidsförvaring. Regeringen framhöll vidare att myndigheterna är rättsligt förpliktade att bevara allmänna handlingar och bevarandet är också en arbetsuppgift av allmänt intresse. Den behandling av icke känsliga personuppgifter som bevarandet utgör är således tillåten enligt artikel 7. För myndigheternas bevarande av känsliga personuppgifter ansågs det däremot behövas ett undantag enligt artikel 8.4, vilket var möjligt enligt direktivet då bevarandet utgör ett viktigt allmänt intresse som berättigar en medlemsstat att göra ett undantag. Att arkivmyndigheter lämnar ut icke sekretessbelagda uppgifter med stöd av offentlighetsprincipen kunde inte heller anses oförenligt med de ändamål för vilka uppgifterna samlades in, framhöll regeringen (prop. 1997/98:44 s. 47 f.).

Bestämmelsen i 10 § arkivlagen om att avvikande bestämmelser om gallring av vissa allmänna handlingar i annan lag eller förordning ska ha företräde framför arkivlagens gallringsregler syftar inte på personuppgiftslagens bestämmelser om hur länge personuppgifter får bevaras. Arkivlagstiftningen har alltså i fråga om allmänna handlingar företräde framför personuppgiftslagens bestämmelser om längsta bevarandetid. I detta avseende kan alltså sägas att intresset av att bevara allmänna handlingar har prioriterats framför integritetsskyddsintresset.

För personuppgifter som inte ingår i allmänna handlingar gäller dock det grundläggande kravet i 9 § första stycket i PuL om att myndigheter inte får bevara personuppgifter under en längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen. Sådana uppgifter ska således avidentifieras eller förstöras eller, med den arkivmässigt relevanta termen, rensas bort när de inte längre behövs. Det torde inte vara aktuellt med fortsatt bevarande av sådana uppgifter för historiska, statistiska eller vetenskapliga ändamål. Om så ändå sker, följer av 2 kap. 9 § TF att handlingarna vari personuppgifterna ingår torde vara att betrakta som allmänna genom att de blivit omhändertagna för arkivering.

Myndigheter har inte exkluderats från den s.k. missbruksregelns tillämpningsområde. Personuppgiftslagens krav i fråga om personuppgifter som inte ingår i allmänna handlingar torde därmed inte nödvändigtvis gälla i fråga om personuppgifter som förekommer hos myndigheter i s.k. ostrukturerat material.

Förslaget till uppgiftsskyddsförordning

Kommissionen

Även i förslaget till allmän uppgiftsskyddsförordning finns bestämmelser om längsta bevarandetid.

I förslagets artikel 5 e anges att personuppgifterna ska förvaras i en form som förhindrar identifiering av den registrerade under längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas; personuppgifter får lagras under längre perioder i den mån som uppgifterna endast behandlas för historiska, statistiska eller vetenskapliga forskningsändamål i enlighet med bestämmelserna och villkoren i artikel 83 och om en periodisk översyn genomförs för att bedöma behovet av fortsatt lagring.

Den sistnämnda artikeln handlar enbart om behandling för historiska, statistiska och vetenskapliga forskningsändamål. Där föreslås bl.a. att personuppgifter får behandlas för historiska, statistiska och vetenskapliga forskningsändamål endast under förutsättning att dessa ändamål inte kan uppfyllas på annat sätt genom behandling av uppgifter som inte medger eller inte längre medger identifiering av den registrerade samt att uppgifter som gör det möjligt att hänföra information till en identifierad eller identifierbar registrerad person ska hållas åtskilda från övrig information så länge som dessa ändamål kan uppfyllas på det sättet. Dessutom får som huvudregel uppgifter inte publiceras eller annars röjas.

Enligt artikel 17 föreslås att den registrerade under vissa förhållanden får en rätt att bli bortglömd och en rätt att utverka radering av personuppgifter som rör vederbörande. Enligt kommissionen är detta en precisering av den rätt till radering som föreskrivs i artikel 12 b i direktivet (se kommissionens förklaring till förordningen, avsnitt 3.4.3.3). Den registeransvarige ska då avstå från ytterligare spridning av sådana uppgifter, särskilt när det gäller personuppgifter som gjordes tillgängliga av den registrerade när vederbörande var barn. Bland annat kan detta gälla om uppgifterna inte längre är nödvändiga för de ändamål för vilka de samlats in eller på annat sätt behandlats. Den registeransvarige ska genomföra en radering utan dröjsmål, utom i den utsträckning som det är nödvändigt att bevara personuppgifterna för bl.a. historiska, statistiska eller vetenskapliga forskningsändamål enligt artikel 83 (artikel 17.3 c) eller för att iaktta en rättslig förpliktelse att bevara personuppgifter enligt unions-

lagstiftningen eller enligt en medlemsstats lagstiftning som den registeransvarige lyder under (artikel 17.3 d). I det sistnämnda fallet krävs dock att medlemsstaternas lagstiftning ska uppfylla ett mål av allmänt intresse, respektera det väsentliga innehållet i rätten till skydd av personuppgifter och vara proportionell mot det legitima mål som eftersträvas.

Europaparlamentet

Europaparlamentet har föreslagit vissa ändringar i förordningen av intresse för bevarandefrågorna. Det föreslås bl.a. att arkivändamål förs in i artikel 5 e som ett lagringsändamål vid sidan om historiska, statistiska eller vetenskapliga forskningsändamål. Vidare föreslås en ändring i artikel 9.2 enligt vilken nödvändig behandling för arkivtjänster tas in som ett nytt undantag från förbudet att behandla känsliga personuppgifter.

Möjligheterna till behandling för arkivtjänster regleras vidare i en av parlamentet föreslagen ny artikel 83 a enligt vilken personuppgifter får, under en längre tid än vad som är nödvändigt för att uppnå syftena med den behandling för vilken uppgifterna samlats in, behandlas av arkivtjänster vilkas huvudsakliga uppgift eller lagstadgade uppgift är att samla in, lagra, tillhandahålla information om, använda och sprida arkivalier i det allmännas intresse, särskilt för att försvara enskildas rättigheter eller för historiska, statistiska eller vetenskapliga forskningsändamål. Dessa uppdrag ska utföras i enlighet med medlemsstaternas bestämmelser om tillgång till och utlämnande och spridning av administrativa handlingar eller arkivhandlingar och i enlighet med bestämmelserna enligt förordningen, särskilt vad gäller samtycke och rätten att göra invändningar.

Några kommentarer

Kommissionens förslag innebär en viss uppstramning när det gäller de allmänna och grundläggande förutsättningarna för att bevara personuppgifter jämfört med motsvarande reglering i dataskyddsdirektivet. Bland annat genom uttryckligt krav på regelbundna omprövningar av behovet av fortsatt lagring av uppgifter om identifierbara personer (artikel 5) och krav på att personuppgifter som be-

varas för historiska, statistiska eller vetenskapliga forskningsändamål om möjligt ska lagras i kodad form åtskilda från den s.k. kodnyckeln (artikel 83). Enligt vår bedömning är det dock inte särskilt troligt att just dessa förslag har direkt betydelse för myndigheternas arkivverksamhet.

Förslaget i artikel 17 om den registrerades rätt att bli bortglömd och utverka radering förefaller ge registrerade, under vissa förhållanden, en rätt till utplåning som kan liknas vid en rätt till gallring. Det verkar dock på nuvarande stadium inte troligt att förslaget får någon omedelbar betydelse för svenska myndigheters bevarande och arkiverande av allmänna handlingar. Det finns skäl att tro att förändringar i kommissionens förslag kommer att skapa ett större utrymme för undantag för den offentliga sektorn och för nationell lagstiftning rörande myndigheternas personuppgiftsbehandling.

14.3 Reglering i registerförfattningar

När stora mängder personuppgifter samlas hos myndigheter uppstår oundvikligen integritetsrisker, i synnerhet då informationsteknikens utveckling inneburit ständigt förbättrade möjligheter till avancerade sök- och sammanställningar av personuppgifter på ganska enkla sätt. Redan då databaserade myndighetsregister började diskuteras i den allmänna debatten uppmärksammades att det var viktigt från integritetssynpunkt att personregister gallrades. I datalagens (1973:289) förarbeten lyftes bl.a. fram som en integritetsrisk att ofördelaktiga uppgifter om en persons förflutna i otillbörlig grad påverkar hans eller hennes möjligheter i framtiden (prop. 1973:33 s. 42 och 129). Enligt datalagen förutsattes Datainspektionen meddela föreskrifter om bl.a. bevarande och gallring även av myndigheters personregister, i den mån det behövdes för att förebygga otillbörliga intrång i den personliga integriteten.

Bakgrunden till utformningen av 10 § tredje stycket arkivlagen om att avvikande bestämmelse om gallring av vissa allmänna handlingar i annan lag eller förordning gäller före arkivlagen är följande. I förarbetena till arkivlagen påpekade föredragande departementschef att man när det gäller bevarande av allmänna handlingar också måste föra in integritetsaspekten. Integritetshänsyn kunde leda till att material inte bevarades i den utsträckning som hade varit önsk-

värd från andra synpunkter eller att tillgången till bevarat material begränsades. Sådana av integritetshänsyn påkallade avvikelser från huvudregeln om bevarande borde dock tas in i de särskilda lagar som reglerar integritetskänsliga akter och register. Reglerna kunde därmed bäst anpassas efter vad det speciella materialet kräver (prop. 1989/90:72 s. 32).

Det finns ingen allmän bestämmelse i arkivlagen om hur integritetsintressena, som talar för gallring, ska vägas mot de intressen som anges i 3 § arkivlagen om arkivens syfte. Den föredragande departementschefen uttalade emellertid i motiven till arkivlagen att bestämmelser i registerförfattningar om gallringsskyldighet som regel bör ges i lag (a. prop. s. 77). Vid sin behandling av regeringens förslag framhöll kulturutskottet nödvändigheten av att göra en avvägning mellan olika intressen när det gäller gallring och att därvid integritetsaspekten är särskilt viktig att beakta. Vidare underströk utskottet att huvudregeln för gallring är att särbestämmelser bör ha lagform, vilket ju hade slagits fast i propositionen. Utskottet delade dock den bedömning som hade gjorts där om att det bör finnas möjlighet att göra undantag från huvudregeln med tanke på att det kan finnas fall då en lagreglering enbart med hänsyn till en gallringsbestämmelse vore onödig (1989/90:KrU29 s. 12 f.).

Vidare konstaterades i motiven till arkivlagen, mot bakgrund av då gällande registerförfattningar, att gallringsbestämmelserna i flertalet registerförfattningar var konstruerade utifrån en omvänd princip i förhållande till den som den föreslagna arkivlagen skulle bygga på, nämligen att gallring ska ske om inte något annat uttryckligen föreskrivits (a. prop. s. 50 f.). Enligt departementschefen var denna omvända princip eller presumtion i förhållande till arkivlagen rimlig med hänsyn till de integritetsintressen som kan föreligga på de särskilda registerförfattningarnas område.

När det däremot gällde undantag från gallringsskyldigheten framhölls att det från lagstiftningsteknisk synpunkt fanns anledning att se något olika på de undantag som kan komma i fråga. Undantag som förestavas av hänsyn till insynsaspekten och myndighetens informationsbehov samt rättssäkerhetsaspekter bör och kan som regel tas in direkt i den särskilda registerlagen. Sådana frågor kan nämligen normalt regleras genom generella bestämmelser. Däremot borde, menade departementschefen, konkreta avgöranden av vilka handlingar som bör bevaras med hänsyn till forskningens behov i

princip överlåtas på fackkunnigt folk inom arkivmyndigheterna. När det gäller bevarande för forskningens behov förordade departementschefen således att det i lagen slogs fast att, utöver de undantag från gallringsplikten som konkret angavs i lagen, ytterligare undantag fick föreskrivas av regeringen eller den myndighet som regeringen bestämde.

I flertalet registerförfattningar finns bestämmelser om bevarande och gallring. Den normala principen för dessa bestämmelser är att presumtionen är omvänd i förhållande till arkivlagens huvudregel om bevarande av allmänna handlingar. I registerförfattningarna föreskrivs normalt att gallring ska ske på vissa sätt, dvs. utgångspunkten är obligatorisk gallring, men att undantag får föreskrivas. Det är vanligt att principen om gallring som huvudregel återfinns i lagen medan det i förordningar som utfärdats i anslutning till registerlagen har överlåtits åt Riksarkivet att meddela närmare föreskrifter om undantag från gallring.

I den mån det i särförfattningar för myndigheters registerföring eller annan behandling av personuppgifter inte finns gallringsbestämmelser, tillämpas däremot arkivlagens bestämmelser om bevarande som huvudprincip och med närmare föreskrifter, som meddelats i anslutning till arkivlagen, om när gallring får ske. Utgångspunkten här är alltså att gallring är en frivillig åtgärd för den arkivbildande myndigheten.

Det kan avslutningsvis noteras att arkivlagstiftningen inte medför några rättigheter för enskilda registrerade. En utebliven obligatorisk gallring enligt en föreskrift i en registerlag torde däremot t.ex. kunna vara i och för sig skadeståndsgrundande enligt 48 § PuL förutsatt att den bestämmelsen även gjorts tillämplig vid personuppgiftsbehandlingen enligt registerlagen i fråga.

Exempel på utformningen av regler om bevarande och gallring i registerförfattningar

Lagen om behandling av personuppgifter om totalförsvarspliktiga

I 15 § lagen (1998;938) om behandling av personuppgifter om totalförsvarspliktiga föreskrivs att en personuppgift i ett automatiserat register över totalförsvarpliktiga ska gallras så snart uppgiften inte längre behövs för de ändamål för vilken behandling får ske enligt

lagen. Gallring är alltså huvudregel och i första hand knuten till lagens ändamålsbestämning. Regeringen får meddela föreskrifter om undantag från gallring i fråga om bevarande av material för forskningens skull. Sådana uppgifter ska dock avföras från registret vid den tidpunkt då de annars skulle ha gallrats enligt lagen. I en anslutande förordning har Riksarkivet bemyndigats att meddela undantag från gallringsbestämmelserna för att tillgodose forskningens behov.

I förarbetena betonade regeringen att gallringsbegreppet används i lagen på samma sätt som enligt Riksarkivets definition och att gallring alltså kan ske genom att uppgifterna förs över på ett annat medium, t.ex. på en mikrofilm, innan de raderas eller utplånas i registret förutsatt att överföringen innebär förlust av möjligheter till informationssammanställningar eller förlorade sökmöjligheter. Dock innebär gallringskravet alltid att personuppgifter ska tas bort från registret. Med tanke på personuppgifternas stora värde för forskning om t.ex. förändringar i folkhälsan fanns dock befogade skäl, menade regeringen, till undantag från gallringskravet. Därmed skulle det inte vara nödvändigt att överföra uppgifterna till annan databärare med någon typ av informationsförlust som följd. Däremot borde personuppgifterna ”avföras, dvs. tas bort från registret”. Vilka uppgifter som ska bevaras med hänsyn till forskningens behov borde Riksarkivet ha att avgöra (prop. 1997/98:80 s. 70 f.).

Lagen om behandling av uppgifter i Kronofogdemyndighetens verksamhet

Enligt de allmänna bestämmelserna i lagen (2001:184) om behandling av uppgifter i Kronofogdemyndighetens verksamhet ska uppgifter som behandlas i någon av Kronofogdemyndighetens olika databaser – utsöknings- och indrivningsdatabasen, betalningsföreläggande- och handräckningsdatabasen, skuldsaneringsdatabasen och konkurstillsynsdatabasen – gallras enligt olika gallringsfrister beroende på till vad för slags ärende uppgifterna hör (2 kap. 6, 12, 18 och 23 §§). I lagen gäller således gallringsskyldighet som huvudprincip. Undantag från den huvudprincipen meddelas av regeringen eller myndighet som regeringen bestämmer.

I förarbetena anfördes att Kronofogdemyndighetens databaser var särskilt integritetskänsliga och att arkivlagens bestämmelser därför

inte borde gälla. I stället borde gallring vara huvudregel med möjlighet för Riksarkivet att föreskriva eller besluta om undantag när det anses motiverat. På så sätt blir det möjligt att ta hänsyn till såväl offentlighets- som integritetsintresset utan en omfattande och tillkrånglad författningsreglering (prop. 2000/01:33 s. 118).

Riksarkivet har alltså bemyndigats att, efter samråd med Kronofogdemyndigheten, meddela föreskrifter om att handlingar och uppgifter får bevaras under längre tid än vad som följer av lagen. Uppgifter och handlingar i skuldsaneringsdatabasen har genom en sådan föreskrift undantagits helt från gallring (RA-MS 2011:29). De ska alltså bevaras. Däremot ska inkommande pappershandlingar i skuldsaneringsprocessen som skannats in i ärendehanteringssystemet gallras. Likartade föreskrifter finns för konkurstillsynsdatabasen (RA-MS 2012:17).

Socialförsäkringsbalken

Enligt 114 kap. 31 § SFB ska personuppgifter gallras när de inte längre är nödvändiga för de primära ändamål som de behandlats för. Regeringen eller myndighet som regeringen bestämmer kan dock meddela föreskrifter om att uppgifter får bevaras för historiska, statistiska eller vetenskapliga ändamål.

I de ursprungliga motiven till föreskrifterna (prop. 2002/03:135 s. 122 f.) gjordes bedömningen att en föreskrift om bevarande för historiska, statistiska och vetenskapliga ändamål innebär bl.a. att rätten att ta del av allmänna handlingar, behovet av information för rättskipningen och förvaltningen samt forskningens behov får beaktas, dvs. de ändamål som arkivlagen syftar till att tillgodose. Riksarkivet har meddelat föreskrifter med relativt omfattande undantag från gallringsskyldigheten.

Det kan nämnas att Lagrådet hade anfört att en huvudregel om gallring utifrån en behovsprövning i förhållande till ändamålen knappast tillförde något utöver vad som följer av 9 § PuL. Av flera skäl ansåg Lagrådet att en tillämpning av arkivlagens bevarande- och gallringsregel i stället vore att föredra, bl.a. eftersom huvudregeln om gallring är så vag att det blir regeringen eller den myndighet som regeringen bestämmer som kommer att ge bestämmelsen innehåll (a prop. s. 165).

Det finns många fler registerförfattningar som på motsvarande sätt föreskriver att bevarande, trots huvudregler om gallring, får ske för historiska, statistiska eller vetenskapliga ändamål som undantag från en huvudprincip om gallring. Här kan noteras att vid angivande av för vilka syften fortsatt bevarande får ske, så är det de ändamål som enligt dataskyddsdirektivet och personuppgiftslagen kan motivera långtidslagring som används och inte något av de ändamål för bevarande av allmänna handlingar som anges i 3 § arkivlagen.

Förordningen om registerföring m.m. vid allmän domstol med hjälp av automatiserad behandling

Uppgifter i elektroniska verksamhetsregister vid allmänna domstolar – som utgör domstolarnas mål- och ärendehanteringssystem – ska alltid gallras inom vissa tidsramar räknade från avgörandeåret. Någon möjlighet till undantag är inte föreskriven. Dock föreskrivs att domstolen innan uppgifterna gallras ska se till att uppgifterna bevaras i skrift, dvs. i form av pappersutskrifter, i den omfattning som Domstolsverket föreskriver, se 5 § förordningen (2001:639) om registerföring m.m. vid allmän domstol med hjälp av automatiserad behandling.

I förslaget till domstolsdatalag föreslås inga gallringsregler utan elektroniskt bevarande av allmänna handlingar ska regleras av arkivlagen, arkivförordningen och Riksarkivets föreskrifter (Ds 2013:10). Övriga personuppgifter som inte är allmänna handlingar – t.ex. en föredragningspromemoria eller ett domsutkast – ska få bevaras så länge det är nödvändigt med hänsyn till ändamålen för behandlingen eller om bevarandet sker för historiska, statistiska eller vetenskapliga ändamål. Skälet till nyordningen i förhållande till gällande rätt motiveras med att domstolsdatalagen ska möjliggöra en ordning med s.k. e-akter vilket kräver en anpassning av regleringen om bevarande och gallring.

I stället för gallring av integritetshänsyn föreslås införandet av ett kompletterande integritetsskydd genom att det meddelas bestämmelser i förordning eller myndighetsföreskrifter om att tillgången till elektroniskt bevarade uppgifter i avslutade mål och ärenden ska begränsas i tid och omfattning och kringgärdas av olika åtgärder. Bland annat anges att uppgifterna, när viss tid gått, ska överföras till ett separat datorsystem för fortsatt bevarande med vissa begränsningar

vad avser t.ex. sökning, direktåtkomst, säkerhet och intern åtkomst (a. a. s. 150 f.). Förslaget i denna del synes vara inspirerat av polisdatalagstiftningens reglering om att personuppgifter som inte ska gallras ska avskiljas från den brottsbekämpande verksamheten när de efter vissa angivna tidsfrister och förutsättningar inte längre får behandlas för brottsbekämpande ändamål, se t.ex. 3 kap. 9–11 §§ jämfört med 2 kap. 12 § andra stycket polisdatalagen (2010:361) (prop. 2009/10:85 s. 203 f). Enligt 19 § polisdataförordningen (2010:1155) ska åtkomsten till avskilda uppgifter och handlingar, dvs. till det digitala arkivet, begränsas till särskilt angivna tjänstemän. Liknande bestämmelser finns bl.a. i 12 § kustbevakningsdataförordningen (2012:146).

Studiestödsdatalagen

Enligt 16 § studiestödsdatalagen (2009:287) ska personuppgifter i ärenden gallras senast inom vissa tidsfrister som är knutna till ärenderelaterade slutpunkter eller registreringsdatum. Riksarkivet får, med undantag från 16 § och efter samråd med Datainspektionen, meddela föreskrifter om bevarande för historiska, statistiska eller vetenskapliga ändamål eller för redovisningsändamål. Centrala studiestödsnämnden, dvs. den arkivbildande myndigheten, får vidare, trots lagens krav på gallring, i enstaka fall besluta att personuppgifter i ett ärende om studiestöd ska bevaras på papper eller annat medium som inte är elektroniskt.

I författningskommentaren till 16 § anförde regeringen att med gallring avses enligt paragrafen att personuppgifterna förstörs så att de inte kan återskapas. Det är alltså inte tillåtet för myndigheten att inför gallringen av de behandlade personuppgifterna föra över dem på annat medium, t.ex. papper. I den allmänna motiveringen anfördes dock att det i enstaka fall kunde finnas behov av ett sådant förfarande, t.ex. i samband med en granskning av ärendet hos myndighet med tillsynsfunktioner eller i fråga om beslut i ett ärende som överklagats och där överprövningen ännu inte är klar (prop. 2008/09:96 s. 73 och 87).

Det kan konstateras att den innebörd som i detta lagstiftningsärende lagts in i begreppet gallring inte framgår av lagtexten. Någon motsvarande reglering om att tillåta utskrifter på papper trots lagens

krav på gallring tycks inte finnas i någon annan nu gällande registerförfattning.

Lagen om behandling av personuppgifter vid Institutet för arbetsmarknads- och utbildningspolitisk utvärdering.

Enligt 14 § lagen (2012:741) om behandling av personuppgifter vid Institutet för arbetsmarknads- och utbildningspolitisk utvärdering ska personuppgifter som utgångspunkt gallras så snart de inte längre behövs för de ändamål som de behandlas för. Av intresse här är 3 och 4 §§ i anslutande förordning (2012:742) som föreskriver att Institutet ska upprätta särskilda rutiner för gallring av de uppgifter som har behandlats i verksamheten. Institutet ska dels efter varje avslutat projekt, dels kontinuerligt pröva vilka uppgifter som kan gallras och vilka uppgifter som måste bevaras för att myndigheterna ska kunna fullgöra sitt uppdrag. Vidare föreskrivs uttryckligen att Riksarkivet – då det är aktuellt att föreskriva undantag från gallringsreglerna – ska väga intresset av att uppgifterna bevaras (forskningens behov) mot behovet av skydd för den enskildes personliga integritet.

Några kommentarer och reflektioner

Exemplifieringen ovan visar att registerförfattningarnas regler om bevarande och gallring inte är enhetligt utformade.

Visserligen kan skillnader vara sakligt motiverade på grund av de speciella förhållandena för personuppgiftsbehandlingen i fråga. Huruvida gallring är huvudprincip eller inte kan ha samband med hur integritetskänslig den reglerade informationshanteringen är eller för vilka ändamål som personuppgiftsbehandlingen sker. Likaså kan skillnader i hur gallringstider är bestämda – till vissa tidsfrister utifrån sakliga förhållanden eller till behovet utifrån ändamålen med personuppgiftsbehandlingen – te sig i sitt sammanhang välgrundade.

Det finns emellertid skillnader i utformningen av regleringen som väcker frågor.

En sådan fråga är att det kan vara svårt att bedöma vad gallring enligt registerförfattningarnas bestämmelser konkret innebär i fråga om faktisk informationsförlust. Med tanke på de många undantag

som har föreskrivits av Riksarkivet är det vidare svårt att skaffa sig överblick över vilka konkreta konsekvenser registerförfattningar med gallring som huvudprincip innebär i kvantitativ och kvalitativ mening för myndigheternas informationstillgångar jämfört med om arkivlagens huvudprincip om bevarande hade varit tillämplig. I exemplen ovan med Kronofogdemyndighetens skuldsaneringsdatabas och konkurstillsynsdatabas är undantagen från registerförfattningens huvudprincip om gallring så omfattande att det i praktiken har skett ett slags återgång till arkivlagstiftningens grundregel om bevarande.

I en del författningar är det vidare oklart om det som åsyftas handlar om ett fullständigt förstörande eller om en partiell gallring som t.ex. innebär att informationen bara tas bort från ett register eller ett ärendehanteringssystem men kommer att bevaras i annan form, på pappersutskrifter eller liknande. Som regel framgår inte av författningarna vad som egentligen avses. Det är vidare ofta oklart om avsikten har varit att helt överlåta den bedömningen åt den arkiv- och personuppgiftsansvariga myndigheten.

I de fall där det i vart fall indirekt framgår om det är fullständig eller partiell gallring som avses harmonierar emellertid reglerna inte med varandra i så måtto att begreppet gallring har olika innebörd i olika författningar. I ett fall behandlas bevarande av pappersutskrifter från elektroniska allmänna handlingar som ett undantag från gallringsplikten. I ett annat fall beskrivs samma förfarande såsom ett moment i den föreskrivna gallringen. Förekomsten av sådana sinsemellan motstridiga regleringar är olycklig och underlättar inte förståelsen om vad som följer av de aktuella regelverken. När det gäller rena begreppsfrågor förefaller det alltså finnas en risk för att den varierande och inte helt enhetliga användningen i registerförfattningar av förekommande begrepp – gallra, förstöra, utplåna, avföra, ta bort – leder till osäkerhet vid tillämpningen.

Vidare förekommer olika varianter av registerförfattningars beskrivningar av för vilka syften personuppgifter ska bevaras, antingen hänvisas till den dataskyddsrättsliga lokutionen ”historiska, statistiska eller vetenskapliga ändamål” eller så hänvisas till arkivens syften enligt 3 § arkivlagen. Om begreppsvalet innebär någon skillnad i sak är emellertid tveksamt. I allt väsentligt överlappar de syften som anges i 3 § arkivlagen personuppgiftslagens motsvarighet och regeringen har i motiven till personuppgiftslagen uttalat att arkiv-

lagens syften ryms inom begreppen historiska, statistiska och vetenskapliga ändamål (prop. 1997/98:44 s. 47). Vissa mindre skillnader finns dock. Exempelvis torde arkivlagens forskningsbegrepp, som i sitt sammanhang inkluderar amatörforskning, vara ett mera vidsträckt ändamål än det som ligger i personuppgiftslagens begrepp vetenskapligt ändamål. Rättsligt sett vållar detta måhända inte några problem eftersom historiska ändamål bör kunna omfatta amatörforskning, t.ex. släktforskning. Man kan dock fråga sig i vad mån bevarande för ”statistiska ändamål” passar ihop med arkivregleringen.

En annan reflektion är att Riksarkivet, till skillnad från vad som förutsattes vid arkivlagens införande, numera har att göra många slags avvägningar mellan integritetsintresset och de olika ändamål för vilka ett fortsatt bevarande kan vara påkallat. Riksarkivets bevakningsområde kan därmed sägas ha vuxit efter hand; från ambitionen vid arkivlagens införande med tonvikt på ansvaret för att verka för att forskningens långsiktiga behov tillgodoses till att också bevaka inte bara allmänhetens rätt till insyn, rättskipningens och förvaltningens behov utan även skyddet av registrerades personliga integritet och ibland även behovet av statistikproduktion.

Slutligen kan anmärkas att det inte sällan anges i registerförfattningar att det är personuppgifter som ska gallras. Rättsligt sett förefaller det kunna uppstå ett glapp mellan vad som ska ske med personuppgifter respektive med vad som får ske med uppgifter om sakförhållanden m.m. som rimligen inte kan anses vara personuppgifter och som kan tänkas förekomma i samma handling eller upptagning. Bedöms det saknas stöd att gallra även sådana övriga uppgifter torde allmänna handlingar få gallras genom att avidentifieras, vilket kan antas vara praktiskt komplicerat och kostsamt. Under alla förhållanden förefaller det inte vara särskilt ändamålsenligt med bestämmelser om gallring enbart av personuppgifter som förekommer i färdiga elektroniska handlingar, t.ex. inlagor som skannats in för lagring i ett elektroniskt ärendesystem.

14.4 Våra överväganden och förslag

14.4.1 Allmänna utgångspunkter

Av redogörelsen i avsnitt 14.1 och 14.2 framgår att regleringen av hur länge personuppgifter får bevaras hos myndigheter är komplex i och med att behandlade personuppgifter så gott som alltid ingår i upptagningar som är eller kommer att bli allmänna handlingar hos myndigheterna. Sådana handlingar omfattas av ett regelverk rörande bevarande som kan sägas ha en diametralt motsatt utgångspunkt mot vad det persondataskyddsrättsliga regelverket har. I det ena fallet är bevarande huvudregeln medan motsatsen gäller i det andra.

I personuppgiftslagen regleras denna konflikt genom bestämmelsen i 8 § andra stycket PuL som innebär att personuppgiftslagens föreskrifter inte hindrar att en myndighet arkiverar och bevarar allmänna handlingar eller att arkivmaterial tas om hand av en arkivmyndighet samt att 9 § fjärde stycket inte gäller för en myndighets användning av personuppgifter i allmänna handlingar, dvs. att personuppgifter i arkiverade handlingar får användas för att vidta åtgärder i fråga om den registrerade. Detta förhållande gäller normalt sett generellt, dvs. för såväl myndighetsverksamhet som omfattas av registerförfattningar som verksamhet som regleras enbart genom personuppgiftslagen. Utgångspunkten kan därmed sägas vara att myndigheters arkivbildning och arkivmyndigheters omhändertagande av arkivmaterial har getts företräde.

Samtidigt förhåller det sig alltså så, att det i många registerförfattningar – både sådana som vi kallar informationshanteringsförfattningar och sådana som rör specifika register – har införts huvudregler om gallring som i väsentlig omfattning modifierar arkivlagstiftningens grundläggande krav på bevarande.

14.4.2 Vilken huvudprincip bör gälla?

Förslag: Arkivlagstiftningens bestämmelser om bevarande och gallring ska gälla enligt den nya lagen vid myndigheters behandling av personuppgifter som ingår i eller kan komma att ingå i allmänna handlingar. Detta ska framgå genom en hänvisning till 8 § andra stycket PuL som alltså ska ha motsvarande

tillämpning vid myndigheters behandling av personuppgifter enligt den nya lagen.

Sedan införandet av arkivlagen har den informationstekniska utvecklingen medfört avsevärda förändringar. Mycket stora informationsmängder samlas numera i myndigheternas datorsystem med alltmer avancerade möjligheter för sökning, bearbetning och sammanställning. Det är givet att den potentiella risken för integritetsintrång ökar med denna utveckling. Även om sekretessreglering finns på mer integritetskänsliga områden kan stora mängder information vara åtkomliga för många hos myndigheterna.

Detta skulle kunna tala för att man på motsvarande sätt som gjorts i flera informationshanteringsförfattningar i den nya lagen om myndigheters personuppgiftsbehandling inför en huvudprincip om att gallring ska ske, dvs. en gallringspresumtion. Det finns dock skäl som med styrka talar emot detta.

Det finns numera i praktiken knappast något alternativ till elektronisk informationshantering och tekniken ger förutsättningar för effektivisering, förbättrad service och ökad rättssäkerhet i myndigheternas verksamhet vilket det är ett starkt samhälleligt intresse att ta tillvara. På motsvarande sätt är det ett starkt samhälleligt intresse att informationstekniken kan tas tillvara för att ge allmänheten insyn i myndigheternas verksamhet liksom att myndigheternas informationssamlingar kan användas som en samhällelig resurs och inte bara för myndigheternas omedelbara behov. Elektronisk primär lagring av information har blivit allt mer vanlig, liksom digital arkivering av allmänna handlingar. Med en elektronisk informationshantering som är en integrerad del av myndigheternas verksamheter på alla nivåer blir den tidigare vanliga ordningen för registerförfattningar med gallring som huvudregel och bevarande som undantag allt svårare att hävda utan allvarliga konsekvenser för offentlighetsinsynen och de övriga intressen som bär upp arkivverksamheten och som anges i 3 § arkivlagen.

Den nya lagen ska kunna tillämpas av ett stort antal statliga och kommunala myndigheter alldeles oavsett karaktären på deras informationshantering och graden av integritetskänslighet i den personuppgiftsbehandling som äger rum. En allmän huvudregel om att personuppgifter i allmänna handlingar ska gallras skulle därför i praktiken behöva förses med så många och omfattande undantag

att den i realiteten skulle komma att sakna egentlig funktion samtidigt som dessa undantagsregler skulle fordra mycket stora arbetsinsatser att ta fram.

Mot den angivna bakgrunden anser vi att en bestämmelse om gallring som huvudprincip när det gäller myndigheters behandling av personuppgifter i allmänna handlingar knappast kan komma i fråga beträffade den nya lagen. I stället ska den arkivrättsliga huvudregeln om bevarande vara grunden för myndigheters behandling av personuppgifter. I den nya lagen bör det därmed, menar vi, komma till uttryck att arkivlagstiftningen gäller för myndigheternas behandling av personuppgifter som ingår i allmänna handlingar.

I registerförfattningar som konstruerats på motsvarande sätt som den vi föreslår – dvs. genom en reglering som ersätter personuppgiftslagen men anger olika bestämmelser i personuppgiftslagen som ändå ska tillämpas – hänvisas utan undantag till 8 § PuL om förhållandet till offentlighetsprincipen, dvs. inbegripet paragrafens andra stycke.

Vi anser att en motsvarande hänvisning bör tas in i den nya lagen. Av hänvisningen följer att varken övriga tillämpliga bestämmelser i personuppgiftslagen eller bestämmelserna i den nya lagen utgör något hinder mot att en myndighet arkiverar och bevarar allmänna handlingar eller att en arkivmyndighet behandlar personuppgifter genom att överta arkivmaterial från en arkivbildande myndighet eller en enskild.

14.4.3 Regler om undantag från huvudregeln om bevarande

Bedömning: Det finns inte anledning att i den nya lagen införa bestämmelser om att viss gallring ska ske.

Det förhållandet att vi inte anser att den nya lagen kan bygga på en presumtion om gallring innebär på inget sätt att gallring av allmänna handlingar skulle sakna betydelse som metod att skydda enskildas personliga integritet.

Vi har därför ställt oss frågan om det finns behov av någon generell gallringsbestämmelse som skulle gälla för alla myndigheter vars personuppgiftsbehandling omfattas av den nya lagen. Vi har emellertid dragit den slutsatsen att så inte är fallet.

Den avvägning som måste göras mellan å ena sidan intresset av bevarande – dvs. intresset av allmänhetens insyn i allmänna handlingar, behovet av information för rättskipningen och förvaltningen, kulturarvsaspekten samt forskningens behov – och, å andra sidan, intresset av gallring med syftet att tillgodose registrerades behov av skydd för sin personliga integritet kan nämligen inte göras utifrån generella utgångspunkter. Avsteg från bevarandepresumtionen i arkivlagstiftningen och därmed från den grundregel som ska gälla vid behandling av personuppgifter enligt den nya lagen bör alltså även i fortsättningen utformas utifrån vad som är påkallat på det särskilda området i fråga efter en ingående och noggrann avvägning mellan de skäl som kan tala för respektive mot bevarande. Det betyder att gallringsbestämmelser måste vara tämligen specifika.

Det ska vidare framhållas att de avvägningar som då ska göras kan vara komplicerade, inte minst därför att det inte är givet att gallring alltid ligger i den registrerades intresse i det långa loppet. Man kan alltså inte alltid utgå från att ett bevarande inte skulle vara av värde för den registrerade. Det kan tvärtom vara av stort värde att kunna få tillgång till arkiverat material för att bringa klarhet i händelseförlopp i handläggningen av ett sedan länge avslutat ärende. Detta intresse kan, men behöver inte, stå i motsats till graden av integritetskänslighet i materialet. Erfarenheterna visar att förekomsten av arkiverade handlingar från höggradigt integritetskänslig verksamhet många år senare kan få mycket stor betydelse för individer vars personuppgifter förekommer i handlingarna.

Av 10 § tredje stycket arkivlagen framgår att från arkivlagen avvikande gallringsbestämmelser i annan lag eller förordning har företräde framför arkivlagen. Det behöver därmed inte föreskrivas i den nya lagen att särskilda gallringsbestämmelser kan gälla i stället för arkivlagstiftningens bestämmelser om bevarande och gallring. En helt annan sak är att sådana särskilda gallringsbestämmelser, i linje med vad vi föreslår beträffande exempelvis särskilda bestämmelser om sökbegränsningar, med fördel kan tas in i en bilaga till den nya lagen eller meddelas i en till den lagen anslutande förordning.

Det kan här erinras om att bestämmelser om gallring i arkivvårdande syfte, dvs. som motiveras av att begränsa arkiven till att omfatta bara det som har ett informationsvärde för framtiden, givetvis också gäller vid myndigheters behandling av personuppgifter. Det följer av arkivlagen eller föreskrifter som meddelats med

stöd av arkivlagen. Arkivlagens bestämmelser kommer därför att gälla parallellt med eventuella särskilda gallringsbestämmelser. På det statliga området finns sådana gallringsföreskrifter som är generella eller myndighetsspecifika och som meddelats av Riksarkivet. Indirekt kan sådana gallringsföreskrifter ha betydelse även för integritetsskyddet och förefaller också tillämpas med den biavsikten. Ett exempel är Riksarkivets föreskrifter och allmänna råd om gallring av handlingar av tillfällig eller ringa betydelse (RA-FS 1991:6; ändrad genom RA-FS 1997:6). Under förutsättning att allmänhetens rätt till insyn inte åsidosätts och att handlingarna bedöms sakna värde för rättskipning, förvaltning och forskning får sådana handlingar gallras av statliga förvaltningsmyndigheter (7 §). E-delegationen har i delbetänkandet Så enkelt som möjligt för så många som möjligt – Bättre juridiska förutsättningar för samverkan och service framhållit att den bestämmelsen kan användas för att besluta om s.k. omedelbar gallring i samband med att enskildas användning av e-tjänster i form av presentationstjänster och hjälptjänster tillfälligt genererar allmänna handlingar vilka bedöms vara av tillfällig betydelse och sakna betydelse från offentlighetssynpunkt (SOU 2014:39 s. 103 f.).

14.4.4 Utformningen av specifika gallringsbestämmelser

Bedömning: Särskilda gallringsbestämmelser bör utformas i enlighet med arkivlagstiftningens terminologi och enbart ta sikte på att begränsa hur länge personuppgifter i allmänna handlingar får bevaras.

De gallringsbestämmelser som behövs till skydd för registrerades integritet vid myndigheters behandling av personuppgifter enligt lagen bör alltså enligt vårt förslag även fortsatt utformas utifrån de speciella behov och det slags intresseavvägningar som uppstår i viss typ av verksamhet eller gäller en viss informationssamling osv.

Det är dock vår bestämda uppfattning att sådana särskilda gallringsregler måste anpassas bättre till arkivlagstiftningens terminologi än vad som är fallet för närvarande. Begreppsbildningen på området behöver stramas upp. Som vi ser det handlar det arkivrättsliga begreppet ”gallring” om arkivvårdande åtgärder, dvs. åtgär-

der som innebär att handlingar inte ska vara kvar i en myndighets arkiv eller aldrig ska hamna där (omedelbar gallring). Vi förordar att den arkivrättsliga termen gallring genomgående används även när det som avses är föreskrifter om att inte längre bevara personuppgifter i allmänna handlingar. Gallringsbegreppet bör således enbart användas i den betydelse som begreppet har i arkivlagstiftningen. En annan sak är att inget hindrar att man i särskilda gallringsföreskrifter också anger hur gallring ska ske, t.ex. om viss partiell gallring avses eller att vissa uppgifter eller handlingar ska förstöras helt eller delvis.

Enligt vår uppfattning bör det vidare inte anges att undantag från gallringsplikt enligt en särskild gallringsregel får meddelas för bevarande för ”historiska, statistiska eller vetenskapliga ändamål”, dvs. med angivande av dataskyddsdirektivets och personuppgiftslagens lokution. De syften som motiverar fortsatt bevarande finns uttryckligt angivna i 3 § arkivlagen. Vi anser att det är till dessa syften hänvisning bör ske, uttryckligen eller genom en paragrafhänvisning. Syftena i 3 § arkivlagen tillämpas generellt och oberoende av om en allmän handling innehåller personuppgifter eller inte. Det skapar, menar vi, förvirring att man fört in en beskrivning från personuppgiftslagen om varför en återgång till handlingsoffentlighetens grundprincip om bevarande kan komma i fråga. Det ger ett felaktigt intryck av att bevarandet sker med stöd av personuppgiftslagen. Att i detta hänseende avvika från direktivets ordalydelse för att i stället använda en redan etablerad nationell begreppsapparat för samma sakförhållande kan inte anses strida mot direktivet enligt vår uppfattning.

14.4.5 Åtgärder för att skydda bevarade personuppgifter

Från integritetssynpunkt är det givetvis inte tillfredsställande om personuppgifter som inte längre behövs i en myndighets verksamhet fortsätter att vara tillgängliga tillsammans med uppgifter som är aktuella i t.ex. ett ärendehanteringssystem som en förhållandevis vid krets av behöriga ärendehandläggare har tillgång till och kanske även andra myndigheters handläggare via direktåtkomst. Verksamhetens behov av en effektiv och enkel tillgång till sådana uppgifter klingar normalt av ju längre tid som gått efter handläggningens

avslutande eller det att en person inte längre är aktuell i en faktisk verksamhet varför en sådan fortsatt lagring och tillgänglighet i myndighetens ordinarie databaser inte alltid ter sig motiverad. Det följer emellertid av den bestämmelse vi föreslagit i avsnitt 10.2.5 om att anställda bara ska ges den tillgång till personuppgifter som krävs för att de ska kunna utföra sina arbetsuppgifter att behörigheten till inaktuella uppgifter inte kan vara obegränsad.

En åtgärd för att motverka integritetsrisker som kan vara förknippade med elektroniskt bevarande av personuppgifter i allmänna handlingar är alltså att se till att personuppgifterna inte är lika åtkomliga när de inte längre är aktuella och behövs för den löpande verksamheten hos myndigheten.

Som har framgått finns det informationshanteringsförfattningar där det förekommer bestämmelser om att personuppgifter ska avskiljas för fortsatt bevarande i myndigheternas elektroniska arkiv, åtskilda från ordinarie informationssamlingar i pågående verksamheter och med en strikt begränsad intern åtkomst. Det förekommer också att Datainspektionen i sin tillsynsverksamhet ställer krav på att personuppgifter ska avskiljas när de inte längre behövs för det ursprungliga ändamålet (se t.ex. Datainspektionens föreläggande mot Försäkringskassan rörande intern åtkomst, beslut 2009-06-23, dnr 1764-2008 eller mot Landstinget Gävleborg, beslut 2014-01-23, dnr 52-2013, rörande provresultat från alkoholtester). Datainspektionen har beskrivit avskiljande som en säkerhetsåtgärd i personuppgiftslagens mening som innebär att personuppgifterna lagras på ett sådant sätt att de inte längre hålls tillgängliga i den dagliga hanteringen (Datainspektionens rapport 2010:2, Intern åtkomst till känsliga personuppgifter hos försäkringsbolag, s. 5).

Det ska observeras att ett avskiljande i nu angiven mening inte utgör en gallring i arkivlagstiftningshänseende. En vanlig metod att avskilja är att uppgifterna förs över till en databas för fortsatt lagring i myndighetens elektroniska arkiv.

Vi har övervägt om det finns skäl att i den nya lagen införa en generell regel rörande åtgärder av det nu aktuella slaget. Vi bedömer dock att behovet och utformningen av sådana bestämmelser måste övervägas och anpassas efter förhållandena på det relevanta området om åtgärderna ska fungera väl, vara flexibla och bara omfatta fall där sådana restriktioner eller begränsningar verkligen är motiverade.

Vi återkommer till begreppet avskiljande i avsnitt 15.4.4.

14.4.6 Personuppgifter som ingår i handlingar som inte är allmänna

Viss information hos myndigheterna blir aldrig allmän handling. Det kan t.ex. handla om sådana minnesanteckningar m.m. som avses i 2 kap. 9 § TF och som aldrig tas om hand för arkivering eller handlingar som är undantagna från att uppnå statusen av att vara allmän handling, t.ex. sådana säkerhetskopior som genereras i myndigheternas verksamhet och som omfattas av ett undantag i 2 kap. 10 § TF. Vi ser ingen anledning att för personuppgifter som ingår i handlingar av det nämnda slaget föreslå någon reglering som ersätter eller avviker från vad som föreskrivs i 9 § första stycket i PuL om längsta bevarandetid. Den bestämmelsen bör alltså vara tillämplig i fråga om personuppgifter som behandlas enligt den nya lagen och som inte ingår i någon allmän handling. Detta följer emellertid redan av vad vi föreslagit i avsnitt 9.2.4 om att 9 § PuL ska vara tillämplig vid personuppgiftsbehandling enligt den nya lagen.

Personuppgiftslagens grundläggande krav innebär alltså att personuppgifter inte får bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen (9 § första stycket i). De får visserligen bevaras längre om det behövs för historiska, statistiska eller vetenskapliga ändamål (9 § andra stycket). Vi bedömer dock att det normalt sett knappast kan bli aktuellt med någon sådan förlängd bevarandetid för just dessa ändamål utan att handlingarna vari personuppgifterna ingår ska anses omhändertagna för arkivering och därigenom bli allmänna handlingar.

Det kan här erinras om att det i 3 § arkivförordningen föreskrivs att myndigheter i samband med att ett ärende slutbehandlas ska ta ställning till om minnesanteckningar, utkast och koncept m.m. som hör till ärendet ska tas om hand för arkivering och bli allmänna handlingar eller om akten eller motsvarande ska rensas från sådana handlingar. Högsta förvaltningsdomstolen har uttalat att det krävs en aktiv åtgärd av myndigheten för att en handling ska anses ha tagits om hand för arkivering. Myndigheten ska t.ex. enligt 3 § arkivlagen ”besluta” att handlingen ska arkiveras. De handlingar som efter en sådan genomgång inte anses ingå i akten men som ändå på något sätt finns kvar – t.ex. i en pärm hos en tjänsteman eller i

dennes dator – torde inte kunna anses omhändertagna för arkivering, RÅ 1999 ref. 36. I prop. 1975/76:160 s. 168 gjorde departementschefen motsvarande bedömning beträffande handling som en tjänsteman ”för eget bruk” sparar i en skrivbordslåda i sitt tjänsterum.

Det kan emellertid inte sällan krävas ganska kvalificerade rättsliga bedömningar för att avgöra om och i så fall när föredragningspromemorior, utkast m.m. som varken arkivlagts eller kastats kan anses ha blivit omhändertagna för arkivering. På motsvarande sätt är det – inte minst i den elektroniska miljön – svårt att ange generella kriterier för när sådana handlingar som inte hör till ett ärende blir allmänna handlingar genom att de anses justerade eller färdigställda enligt 2 kap. 7 § TF, detta trots en relativt riklig rättspraxis på området.

Oavsett hur det förhåller sig med detta kan emellertid konstateras att i den utsträckning personuppgifter förekommer i handlingar som inte är allmänna hos myndigheten följer, som framgått, ett krav på den personuppgiftsansvariga myndigheten att ha en överblick över myndighetens totala personuppgiftshantering och aktivt se till – genom t.ex. ändamålsenliga rutiner och uppföljande kontroller – att behandling genom t.ex. fortsatt lagring av för myndigheten inaktuella personuppgifter, som inte ingår i allmänna handlingar, inte pågår utan att det är befogat för det specifika ändamålet med behandlingen. Det är alltså ett dataskyddsrättsligt krav som gäller utöver sådana andra krav som kan gälla för myndigheten om att t.ex. hålla nere volymen på myndighetens elektroniskt lagrade information.

15 Skyldighet att vidta åtgärder då personuppgifter är oriktiga eller behandlas otillåtet

15.1 Allmänna dataskyddsrättsliga regler

Dataskyddsdirektivet

I artikel 6.1 dataskyddsdirektivet finns principer om personuppgifters kvalitet. Där sägs i punkt c att uppgifter ska vara adekvata och relevanta och inte får omfatta mer än vad som är nödvändigt med hänsyn till de ändamål för vilka de har samlats in och för vilka de senare har behandlats. Vidare anges i punkt d att medlemsstaterna ska föreskriva att personuppgifter ska vara riktiga och, om nödvändigt, aktuella. Alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga eller ofullständiga i förhållande till de ändamål för vilka de samlades in eller för vilka de senare behandlas utplånas eller rättas.

Enligt artikel 12 b ska medlemsstaterna säkerställa att varje registrerad har rätt att från den registeransvarige i förekommande fall få sådana uppgifter som inte behandlats i enlighet med bestämmelserna i detta direktiv rättade, utplånade eller blockerade, särskilt om dessa är ofullständiga eller felaktiga.

I artikel 12 c föreskrivs en underrättelseskyldighet som innebär att den registrerade har rätt att ”få genomfört” att en tredje man till vilka sådana uppgifter har utlämnats ska underrättas om varje rättelse m.m. som utförts i enlighet med punkt b, om detta inte visar sig vara omöjligt eller innebär en oproportionerligt stor ansträngning.

Medlemsstaterna ges i artikel 13 rätt att under vissa förutsättningar begränsa de rättigheter som anges i artikel 12. I 13.1 före-

skrivs att medlemsstaterna får genom lagstiftning vidta åtgärder för att begränsa omfattningen av de skyldigheter och rättigheter som anges i artikel 12 i de fall då sådan begränsning är en nödvändig åtgärd med hänsyn till a) statens säkerhet, b) försvaret, c) allmän säkerhet, d) förebyggande, undersökning, avslöjande av brott eller åtal för brott eller av överträdelser av etiska regler som gäller för lagreglerade yrken, e) ett viktigt ekonomiskt eller finansiellt intresse hos en medlemsstat eller hos EU, inklusive monetära frågor, budgetfrågor och skattefrågor, f) en tillsyns-, inspektions- eller regleringsfunktion som, även om den är av övergående karaktär, är förbunden med myndighetsutövning i de under punkterna c), d) och e) nämnda fallen, g) skydd av den registrerades eller andras fri- och rättigheter.

Personuppgiftslagen

Allmänt om bestämmelserna om rättelse

I personuppgiftslagen har bestämmelserna i artikel 6.1 genomförts genom bestämmelserna i 9 § om grundläggande krav på behandling av personuppgifter. Där sägs att den personuppgiftsansvarige ska se till att de personuppgifter som behandlas är adekvata och relevanta i förhållande till ändamålen med behandlingen (punkt e). De ska också vara är riktiga och, om nödvändigt, aktuella (punkt g). Den personuppgiftsansvarige ska vidta alla rimliga åtgärder för att rätta, blockera eller utplåna sådana personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålen med behandlingen (punkt h).

Artiklarna 12.1 b och c har genomförts genom 28 § personuppgiftslagen. I den bestämmelsen föreskrivs att den personuppgiftsansvarige är skyldig att på begäran av den registrerade snarast rätta, blockera eller utplåna sådana personuppgifter som inte har behandlats i enlighet med lagen eller föreskrifter som har utfärdats med stöd av den. Den personuppgiftsansvarige ska också underrätta tredje man till vilken uppgifterna har lämnats ut om åtgärden, om den registrerade begär det eller om mera betydande skada eller olägenhet för den registrerade skulle kunna undvikas genom en underrättelse. Någon sådan underrättelse behöver dock inte lämnas, om det visar sig vara omöjligt eller skulle innebära en oproportionerligt stor arbetsinsats.

Den svenska bestämmelsen innehåller, till skillnad från dataskyddsdirektivet, ett krav på att en rättelse ska vidtas snarast. Även skyldigheten för den personuppgiftsansvarige att under vissa förutsättningar underrätta tredje man om att en korrigering har skett, även om den registrerade inte har begärt det, är en inhemsk reglering som inte krävs enligt direktivet.

Bestämmelserna i artikel 13 i direktivet föranledde ingen reglering i samband med att personuppgiftslagen infördes. Däremot har år 2007 införts en ny bestämmelse i lagen – 8 a § – där regeringen bemyndigas att meddela föreskrifter om undantag från bl.a. 28 §, om det är nödvändigt med hänsyn till de intressen som räknas upp. Dessa motsvarar de intressen som omfattas av artikel 13.

Skyldigheten att rätta m.m.

I förarbetena till personuppgiftslagen (prop. 1997/98:44 s. 86 f.) påpekas att det redan av de grundläggande kraven, dvs. bestämmelserna i 9 §, framgår att den personuppgiftsansvarige på egen hand måste vara aktiv för att se till att behandlade uppgifter är korrekta. Dessa bestämmelser innehåller således en skyldighet för denne att agera. Bestämmelsen i 28 § innehåller en rätt för den registrerade att begära att den personuppgiftsansvarige rättar en uppgift. Det understryks att dataskyddsdirektivet kräver att båda bestämmelserna införs. Eftersom det inte framgår vilken av de alternativa metoderna rättelse, blockering eller utplånande som ska väljas, anses det stå den personuppgiftsansvarige fritt att välja metod.

Det diskuteras inte i förarbetena vad den personuppgiftsansvariges skyldighet att rätta uppgifter närmare består i. Frågan om vad direktivet innebär för myndigheters skyldighet att rätta personuppgifter, exempelvis i förhållande till redan befintliga föreskrifter som kan ha betydelse för frågan, diskuteras inte heller i förarbetena utom i ett avseende. Det gäller myndigheters skyldighet att rätta personuppgifter i allmänna handlingar. I detta sammanhang påpekas att friheten att välja metod för att rätta innebär att direktivet inte kräver att myndigheter utplånar felaktiga uppgifter till förfång för allmänhetens rättigheter enligt offentlighetsprincipen (a. prop. s. 47).

Underrättelseskyldigheten

Som exempel på fall då den personuppgiftsansvarige, oavsett om det finns en begäran från den enskilde, är skyldig att underrätta tredje man om en rättelse nämns i förarbetena att en känslig personuppgift felaktigt har registrerats, t.ex. att den registrerade är sjuk eller har en extrem politisk eller religiös övertygelse (prop. 1997/98:44 s. 134 f.). En sådan registrering sägs regelmässigt kunna antas orsaka sådan skada eller olägenhet som avses. Gäller det däremot en mer harmlös uppgift, t.ex. om den registrerades adress, bör det som regel krävas någon särskild omständighet för att en skada eller olägenhet kan antas uppstå om någon underrättelse inte sker.

Av 28 § följer att underrättelse inte i något fall behöver lämnas om det visar sig vara omöjligt att underrätta eller det skulle innebära en oproportionerlig stor arbetsinsats. I förarbetena diskuteras inte närmare när en sådan undantagssituation kan tänkas vara för handen.

Förslaget till uppgiftsskyddsförordning

I förslaget till en allmän uppgiftsskyddsförordning finns i artikel 6 bestämmelser som motsvarar principerna i artikel 6 i dataskyddsdirektivet om personuppgifters kvalitet. Bland annat sägs i punkten c att personuppgifterna ska vara adekvata, relevanta och begränsade till ett strikt minimum när det gäller de syften för vilka de behandlas; de ska bara behandlas om, och så länge som, syftena inte kan uppnås genom att man behandlar information som inte rör personuppgifter. Vidare föreskrivs i punkten d att personuppgifterna ska vara riktiga och aktuella; alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål.

I artikel 16 finns bestämmelser om rätt till rättelse. Enligt artikeln ska den registrerade ha rätt att av den personuppgiftsansvarige få rättelse av personuppgifter som rör vederbörande och som är felaktiga. Den registrerade ska också ha rätt att få till stånd komplettering av ofullständiga personuppgifter, bl.a. genom att lägga till en korrigering.

I artikel 17 finns bestämmelser om ”rätt att bli bortglömd” och till radering. Där föreskrivs i 17.1 att den registrerade ska ha rätt att

under vissa förutsättningar få personuppgifter som rör denne raderade och att man avstår från ytterligare spridning av sådana uppgifter. Det gäller särskilt när det avser personuppgifter som gjordes tillgängliga av den registrerade när denne var barn. En av följande grunder ska vara tillämplig för att radering ska ske:

a) Uppgifterna är inte längre nödvändiga för de ändamål för vilka de samlats in eller på annat sätt behandlats.

b) Den registrerade återkallar ett samtycke eller den lagringsperiod för vilket samtycke lämnats har löpt ut, och det inte finns någon annan rättslig grund för behandlingen.

c) Den registrerade invänder mot behandlingen enligt artikel 19.

d) Behandlingen uppfyller inte villkoren i förordningen av andra skäl.

En skyldighet att underrätta ”tredje part” framgår av artikel 17.2 och gäller den registrerades begäran om att radera eventuella länkar eller kopior eller reproduktioner av personuppgifter som avses i 17.1.

Av artikel 17.3 följer att den registeransvarige ska genomföra raderingen utan dröjsmål, utom i den utsträckning som det är nödvändigt att bevara personuppgifterna av följande skäl:

a) För att utöva rätten till yttrandefrihet enligt artikel 80.

b) Av viktiga skäl på folkhälsoområdet enligt artikel 81.

c) För historiska, statistiska eller vetenskapliga forskningsändamål enligt artikel 83.

d) För att iaktta en rättslig förpliktelse att bevara personuppgifter enligt unionslagstiftningen eller enligt en medlemsstats lagstiftning som den registeransvarige lyder under; medlemsstaternas lagstiftning ska uppfylla ett mål av allmänt intresse, respektera det väsentliga innehållet i rätten till skydd av personuppgifter och vara proportionell mot det legitima mål som eftersträvas.

e) I de fall som avses i punkt 4.

I artikel 17.4 anges fyra situationer då den registeransvarige ska begränsa behandlingen av personuppgifter i stället för att radera dem, exempelvis då de måste bevaras för bevisändamål (b) eller den registrerade motsätter sig en radering även om behandlingen är

olaglig. Av 17.5 följer att sådana personuppgifter som avses i punkt 4 får behandlas endast för vissa särskilt uppräknande ändamål, bl.a. för att skydda annan fysisk eller juridisk persons rättigheter eller för ett mål av allmänt intresse.

Vad som i detalj kan komma att gälla framgår emellertid inte av uppgiftsskyddsförordningen, eftersom kommissionen enligt artikel 17.9 föreslås få befogenhet att anta delegerade rättsakter i syfte att närmare precisera vad som ska gälla enligt punkterna 1, 2 och 4. Denna befogenhet gäller emellertid inte möjligheterna att bevara personuppgifter enligt punkten 3.

Enligt artikel 13 ska den registeransvarige underrätta varje mottagare till vilken uppgifter har lämnats ut om eventuella rättelser eller raderingar som utförts i enlighet med artiklarna 16 och 17, om inte detta visar sig vara omöjligt eller inbegripa en oproportionerlig ansträngning. Till skillnad från direktivet omfattar skyldigheten inte bara underrättelse till tredje män utan även gemensamma registeransvariga och registerförare.

I Europaparlamentets resolution med ändringsförslag föreslås inga ändringar i artikel 16 om rättelse men däremot i artikel 17 om rätten till radering. Bland annat föreslås i artikel 17.1 att den registeransvarige också ska vara skyldig att radera om det finns ett lagakraftvunnet avgörande från en domstol eller en regleringsmyndighet i unionen. Beträffande artikel 17.2 föreslås att det inte bara ska finnas en underrättelseskyldighet utan att den registeransvarige även ska vidta alla rimliga åtgärder för att få uppgifterna raderade genom tredje parts försorg. Huvudregeln i artikel 17.3 att raderingen ska genomföras utan dröjsmål gäller enligt förslaget därför också för tredje man.

15.2 Reglering i registerförfattningar

Den vanligaste formen av reglering

Bestämmelserna om rättelse och underrättelse till tredje man i 28 § PuL gäller inte om personuppgifter behandlas med stöd av en särskild registerförfattning som gäller före personuppgiftslagen (jfr 2 §). Särskilda registerförfattningar måste därför innehålla egna sådana bestämmelser. Ofta har frågan om rättelse reglerats genom en hänvisning till 28 § personuppgiftslagen (Öman/Lindblom, s. 420).

Som exempel kan nämnas 3 kap. 3 § lagen (2001:181) om behandling av uppgifter i Skatteverkets beskattningsverksamhet.

Särskilda bestämmelser om rättelse

Det förekommer emellertid författningar som innehåller särskilda bestämmelser om rättelse. Som exempel kan nämnas lagen (2011:1200) om elcertifikat. Den innehåller bl.a. bestämmelser om behandling av uppgifter i elcertifikatregistret, för vilket Svenska Kraftnät är personuppgiftsansvarigt (3 kap. 17 § nämnda lag och 3 § förordningen [2011:1480] om elcertifikat). Enligt 3 kap. 15 § ska en uppgift på ett certifikatkonto rättas, om den innehåller någon uppenbar oriktighet till följd av skrivfel, räknefel eller liknande förbiseende eller till följd av något tekniskt fel. Den vars rätt berörs ska ges möjlighet att yttra sig, om rättelsen inte är till förmån för denne eller yttrandet annars är uppenbart obehövligt. Bestämmelsen avviker således från 28 § personuppgiftslagen genom att dels det ställs upp ett krav på att felet ska vara uppenbart, dels att yttrande i vissa fall ska inhämtas. Som skäl för att ha en avvikande bestämmelse om rättelse anfördes i förarbetena till den tidigare lagen (2003:113) om elcertifikat, vars bestämmelse om rättelse motsvarar den nuvarande (prop. 2002/30:40 s. 89 f.) att syftet inte var att skydda den personliga integriteten. Det var i stället att registret på ett korrekt sätt ska återge kontohavarens äganderätt och förfoganderätt till de elcertifikat som finns registrerade på certifikatkonto. Begränsningarna i rättelsebestämmelsens tillämplighet ansågs förenliga med dataskyddsdirektivet, eftersom artikel 13.1 g medger att omfattningen av rätten till rättelse begränsas med hänsyn till skyddet för den registrerades eller andras fri- och rättigheter. Eftersom bestämmelsen avser att skydda bl.a. enskilds äganderätt ansågs de begränsningar som den innefattar omfattas av undantaget i direktivet.

Rättelse i Kronofogdemyndighetens verksamhet

I lagen (2001:184) om behandling av personuppgifter i Kronofogdemyndighetens verksamhet har det år 2008 införts en särskild bestämmelse om rättelse. Enligt 3 kap. 3 a § ska Kronofogdemyn-

digheten på begäran av den registrerade snarast rätta, blockera eller utplåna sådana uppgifter som 1) inte har behandlats i enlighet med lagen eller anslutande författningar, eller 2) är missvisande i fråga om den registrerades vilja eller förmåga att uppfylla sina ekonomiska förpliktelser. Skyldigheten att rätta omfattar både personuppgifter och andra uppgifter (jfr 1 kap. 1 § andra stycket). Bestämmelsen innehåller också regler om underrättelse till tredje man som i sak överensstämmer med 28 § personuppgiftslagen.

I praxis hade det, inte minst efter personuppgiftslagens införande, utvecklats en restriktiv praxis när det gällde att rätta uppgifter i utsöknings- och indrivningsdatabasen (prop. 2007/08:116 s. 12 f.). Detta motiverades främst av att databasen används för såväl målhantering som diarieföring. Frågan om rättelse hade kommit att prövas av domstol i ett stort antal fall. Genom Datainspektionens granskningar hade det också kommit fram att de dåvarande regionala kronofogdemyndigheterna tolkade skyldigheten att rätta på olika sätt. I förarbetena till den nuvarande bestämmelsen om rättelse konstaterades vidare att det sällan är komplicerat att fastställa att en uppgift är oriktig till sitt innehåll, medan bedömningen av om i och för sig riktiga personuppgifter behandlats i strid med personuppgiftslagen emellertid kan erbjuda större svårigheter (a. prop. s. 14 f.) Det senare borde enligt Högsta förvaltningsdomstolen bedömas bl.a. mot bakgrund av ändamålen med databasen och vilka uppgifter som får behandlas (se RÅ 2006 ref. 86). Regeringen anförde att den dåvarande situationen fick antas ha uppkommit till stor del på grund av att det finns flera olika perspektiv som kan anläggas på frågan. Man stannade för att föreslå en lösning som innebar att begreppet ”missvisande”, som förekommit i den tidigare datalagen, skulle återinföras i lagtexten. Regeringen påpekade att det kunde diskuteras om förslaget innebar en utvidgning av skyldigheten att vidta rättelse eller bara ett förtydligande av vad som redan gällde. Något svar lämnades emellertid inte, utan regeringen anförde att det viktigaste var att ändringen, tillsammans med den utbyggnad av sekretesskyddet som också föreslogs, banade väg för en tillämpning som tillgodoser såväl kraven på Kronofogdemyndighetens diarieföring som de enskildas berättigade krav på att inte behöva förekomma med uppgifter som ger ett i sak ogrundat intryck av bristande vilja eller förmåga att göra rätt för sig.

Bestämmelsen om rättelse i dess nuvarande lydelse har prövats av Högsta förvaltningsdomstolen i rättsfallet HFD 2011 ref. 45.

Rättelse enligt 26 § förvaltningslagen i stället för 28 § personuppgiftslagen

Det förekommer att det i förordningsbestämmelser om förande av vissa register föreskrivs att 26 § förvaltningslagen (1986:223) ska tillämpas i stället för 28 § personuppgiftslagen. Som exempel kan nämnas rättelse i aktiebolagsregistret. Enligt 27 kap. 1 § aktiebolagslagen (2005:551) ska Bolagsverket föra ett aktiebolagsregister för registrering enligt lagen eller annan lag. I 2 kap. aktiebolagsförordningen (2005:559) finns bestämmelser om behandlingen av uppgifter i registret. I 6 § föreskrivs att i fråga om rättelse av personuppgifter i aktiebolagsregistret tillämpas 26 § förvaltningslagen i stället för 28 § personuppgiftslagen.

15.3 Förvaltningslagens bestämmelser om rättelse m.m.

Allmänt om bestämmelserna

Enligt 26 § förvaltningslagen får ett beslut som innehåller en uppenbar oriktighet till följd av myndighetens eller någon annans skrivfel, räknefel eller liknande förbiseende rättas av den myndighet som har meddelat beslutet. Innan rättelse sker ska myndigheten ge den som är part tillfälle att yttra sig, om ärendet avser myndighetsutövning mot någon enskild och åtgärden inte är obehövlig.

I 27 § föreskrivs att om en myndighet finner att ett beslut, som den har meddelat som första instans, är uppenbart oriktigt på grund av nya omständigheter eller av någon annan anledning, ska myndigheten ändra beslutet, om det kan ske snabbt och enkelt och utan att det blir till nackdel för någon enskild part. Skyldigheten gäller även om beslutet överklagas, såvida inte klaganden begär att beslutet tills vidare inte ska gälla (inhibition). Däremot gäller skyldigheten inte, om myndigheten har överlämnat handlingarna i ärendet till en högre instans eller om det finns särskilda skäl mot att myndigheten ändrar beslutet.

Av 21 § följer en underrättelseskyldighet för myndigheten. Den innebär (enligt första stycket) att myndigheten ska underrätta en sökande, klagande eller annan part om innehållet i det beslut varigenom myndigheten avgör ärendet, om detta avser myndighetsutövning mot någon enskild. Parten behöver dock inte underrättas, om det är uppenbart obehövligt. I andra stycket finns föreskrifter i fråga om överklagande. Vidare sägs i tredje stycket att myndigheten bestämmer om underrättelsen ska ske muntligt, genom vanligt brev, genom delgivning eller på något annat sätt. Underrättelsen ska dock alltid ske skriftligt, om part begär det. Paragrafen tillämpas också när någon annan som får överklaga beslutet begär att få ta del av det (fjärde stycket).

Närmare om rättelse enligt 26 §

Myndighetens möjlighet att vidta rättelse enligt 26 § FL gäller alla former av ärenden och inte endast då det är fråga om myndighetsutövning. Möjligheten tar enbart sikte på s.k. förbiseendefel, t.ex. vid namnförväxlingar, då belopp har summerats felaktigt, att text i beslut har fallit bort på grund av ett tekniskt missöde eller att myndigheten har förväxlat en sökande med någon annan som gjort en liknande ansökan (Hellners/Malmqvist, kommentaren till 26 §). Befogenheten att rätta gäller även fel som har orsakats av någon annan än myndigheten själv. I förarbetena pekas bl.a. på den situationen att part eller någon annan lämnat en oriktig uppgift om en detalj som är väsentlig för verkställigheten av myndighetens beslut men som inte är tvistig, t.ex. en uppgift om personnummer, adress eller bilnummer (prop. 1989/90:71 s. 50).

Paragrafen ger däremot inte myndigheter någon befogenhet att rätta sådana fel i ett besluts innehåll som beror på en felaktig bedömning, t.ex. på grund av en bristfällig utredning, felaktig bedömning av fakta, oriktig rättstillämpning eller missriktad användning av skönsbefogenheter (bedömningsfel).

Ordet ”får” i paragrafen innebär visserligen en befogenhet att rätta. Det ligger emellertid i sakens natur att myndigheten ska använda sig av denna befogenhet när felet har en praktisk betydelse i något avseende (Hellners/Malmqvist, a.a.). Har en part uttryckligen begärt att ett fel ska rättas, bör myndigheten gå med på

dennes begäran, även om myndigheten har fog för att inte själv ta initiativ till en rättelse t.ex. på grund av att felet rör stavning av namn eller något annat som saknar praktisk betydelse.

Då myndighetens beslut avser myndighetsutövning är ett minimikrav vid rättelse att den som är part ska få tillfälle att yttra sig, om det inte är obehövligt.

Motsvarande möjlighet att rätta oriktiga uppgifter finns också för domstolar i 17 kap. 15 § RB och 32 § FPL.

Närmare om omprövning av beslut enligt 27 §

Om en myndighet har meddelat ett beslut som visar sig vara uppenbart oriktigt, följer av 27 § FL att myndigheten ska meddela ett nytt beslut som upphäver eller ändrar det tidigare beslutet. Här är således inte fråga om att – som sker enligt 26 § – rätta en uppgift i det redan meddelade beslutet, utan att ersätta detta beslut med ett nytt beslut.

Som en förutsättning för att myndigheten ska vara skyldig att ändra sitt beslut gäller att det är lätt för myndigheten att konstatera att beslutet är oriktigt, dvs. någon mer ingående granskning av beslutet bör normalt inte behövas. Bara i det fall då en genomläsning av beslutet visar att det sannolikt är oriktigt, behöver myndighet i allmänhet granska ärendet närmare (prop. 1985/86:80 s. 78). Uttrycket ”uppenbart oriktigt” täcker även det fall då beslutet var riktigt vid tillkomsten, men omständigheter som inträffat senare gör att beslutet framstår som felaktigt eller olämpligt.

En annan förutsättning är att beslutet kan ändras snabbt och enkelt. Skyldigheten att ompröva gäller därför normalt inte när det krävs att ytterligare utredning görs i ärendet (a. prop. s. 78). Slutligen gäller att ändringen ska kunna ske utan nackdel för någon enskild part.

Skyldigheten att ompröva gäller inte då någon som överklagat beslutet begärt att det överklagade beslutet inte ska gälla tills vidare (inhibition), då myndigheten har överlämnat handlingarna i ärendet till en högre instans eller då något annat särskilt skäl talar emot att myndigheten ändrar beslutet.

Skyldigheten att ompröva enligt denna paragraf ska ses som ett minimikrav. Den ska inte förväxlas med de befogenheter att om-

pröva beslut som myndigheter har i enlighet med regler om förvaltningsbesluts rättskraft som har vuxit fram i praxis. Dessa regler ger alltså myndigheter rätt att ompröva sina beslut också i vissa andra fall än då omprövning ska ske enligt förvaltningslagen (denna praxis redovisas inte utförligare här, se vidare Hellners/Malmqvist, kommentaren till 27 § och SOU 2010:29 s. 559 f.). Skyldigheten att ompröva enligt 27 § FL ska inte heller förväxlas med den obligatoriska omprövning som vissa myndigheter är skyldiga att vidta enligt särskilda regler, se t.ex. 113 kap. 7 § SFB.

Närmare om underrättelseskyldigheten

Någon skyldighet att underrätta part om en rättelse som vidtas enligt 26 § FL finns inte. Av bestämmelsen följer emellertid, som redovisats ovan, en skyldighet att låta part yttra sig innan rättelse sker, om det inte är obehövligt. Däremot anses det lämpligt att rättelsen antecknas på den handling som innehåller originalbeslutet samt att datum anges och att rättelsen undertecknas. Myndigheten bör också se till att få tillbaka de exemplar av beslutet som har expedierats och att nya, rättade versioner expedieras (Hellners/Malmqvist, kommentaren till 26 §).

Då myndigheten ändrar ett felaktigt beslut med stöd av 27 § FL och alltså meddelar ett nytt beslut som ersätter det tidigare, följer av 21 § samma lag att en sökande, klagande eller annan part ska underrättas om innehållet i det nya beslutet. Skyldigheten gäller dock inte om det är uppenbart obehövligt att en underrättelse sker.

Förslaget i betänkandet En ny förvaltningslag (SOU 2010:29)

I betänkandet med förslag till en ny förvaltningslag (SOU 2010:29) sägs det vara en brist att det i allt väsentligt inte är reglerat vad som gäller i fråga om myndigheters möjligheter eller skyldigheter att ompröva eller ändra sina egna beslut, förutom i de fall som regleras i 26 och 27 §§ FL och där resultatet enligt utredningen närmast kan betraktas som ”givet” (s. 579 f.). Utredningen föreslår därför en utökad reglering av institutet och använder där genomgående begreppet ”rättelse”.

Utredningen föreslår att det för det första införs en bestämmelse som uttryckligen ger en myndighet obegränsad befogenhet att rätta ett beslut innan det expedierats eller på annat sätt gjorts tillgängligt för utomstående.

Efter denna tidpunkt föreslås beslut kunna rättas under de förutsättningar som anges i lagen. Därvid föreslås en möjlighet att vidta rättelse på grund av skrivfel eller liknande som i allt väsentligt överensstämmer med nuvarande 26 § FL.

Därutöver föreslås en bestämmelse som föreskriver i vilka fall rättelse får ske i andra fall. I bestämmelsen ges en generell befogenhet för en myndighet att rätta sina egna beslut som är felaktiga på grund av att nya omständigheter har tillkommit eller av någon annan anledning. Är beslutet gynnande för någon enskild part får dock rättelse ske endast under vissa omständigheter. Möjligheten att ändra övergår enligt bestämmelsen till en skyldighet, om beslutet är uppenbart ogiltigt i något väsentligt avseende, korrigeringen kan ske snabbt och enkelt och utan att det blir till nackdel för någon enskild part. Särskilda begränsningar gäller för möjligheten att rätta beslut som överklagats.

Vidare föreslås en skyldighet att ge part möjlighet att yttra sig innan rättelse sker, om det inte är uppenbart obehövligt. Skyldigheten föreslås således gälla generellt och inte vara begränsad – som enligt nuvarande 26 § – till ärenden om myndighetsutövning. Det hänvisas också till att det framgår av en annan bestämmelse att part ska underrättas om det beslut som ersätter det rättade.

Förslaget till en ny förvaltningslag har ännu inte lett till någon lagstiftning.

15.4 Våra överväganden och förslag

15.4.1 Det behövs bestämmelser om rättelse m.m. av personuppgifter som kompletterar reglerna i förvaltningslagen

Bedömning: Förvaltningslagens bestämmelse om rättelse och om omprövning av beslut uppfyller inte dataskyddsdirektivets krav på en rätt för den registrerade att begära rättelse eller annan korrigering av personuppgifter som behandlas i strid med direktivet. Kompletterande regler behöver därför finnas beträffande myndigheters behandling av personuppgifter.

Rättelse av oriktiga uppgifter

Av redovisningen ovan framgår att det finns bestämmelser i förvaltningslagen som ger myndigheterna möjlighet att i alla slags ärenden rätta beslut som innehåller en uppenbar oriktighet, t.ex. p.g.a. skrivfel, räknefel eller liknande förbiseenden (26 §), samt att ändra ett beslut som är uppenbart oriktigt p.g.a. nya omständigheter eller av någon annan anledning (27 §).

Bestämmelsen om rättelse i 26 § förvaltningslagen innebär en befogenhet för myndigheterna att vidta rättelse. Någon uttrycklig skyldighet att rätta en uppenbar oriktighet finns dock inte, inte ens i det fallet att en part uttryckligen har begärt att rättelse ska ske. Bestämmelsen innebär inte heller någon uttrycklig rätt för en part att begära att en uppgift ska rättas. Även om det ligger i sakens natur att myndigheten ska använda sig av sin befogenhet att rätta när en felaktig uppgift har en praktisk betydelse i något avseende, kan det alltså konstateras att 26 § varken innebär någon uttrycklig skyldighet för myndigheten eller någon egentlig rätt för part i ett ärende hos myndigheten. Denna omständighet innebär en avgörande skillnad i förhållande till personuppgiftslagens bestämmelser om dels de grundläggande krav i fråga om personuppgifters kvalitet som den personuppgiftsansvarige är skyldig att iaktta när personuppgifter behandlas (9 §), dels den registrerades rätt att begära att den personuppgiftsansvarige rättar oriktiga personuppgifter (28 §).

Av artikel 12 b i dataskyddsdirektivet följer en skyldighet för medlemsstaterna att säkerställa att varje registrerad har rätt att från

den registeransvarige i förekommande fall få personuppgifter rättade m.m., särskilt om dessa är ofullständiga eller felaktiga. Det kan konstateras att denna skyldighet för Sverige som medlemsstat knappast kan anses uppfylld genom 26 § förvaltningslagen, eftersom den bestämmelsen varken innebär någon uttrycklig skyldighet för myndigheten eller en rätt för den registrerade när det gäller att rätta oriktiga personuppgifter i myndigheternas informationssamlingar. Bestämmelsen tar vidare enbart sikte på frågan om rättelse av uppgifter i beslut och inte på när uppgifter hanteras i myndighetens verksamhet i övrigt. Skälet till det torde vara att det anses självklart att en myndighet har befogenhet att rätta felaktiga uppgifter som behandlas i andra sammanhang än i beslut. Det kan emellertid konstateras att det inte heller i det fallet finns vare sig någon uttrycklig skyldighet för myndigheten att rätta eller en rätt för en part att begära att rättelse ska ske. Förvaltningslagens bestämmelse om rättelse av oriktiga uppgifter kan alltså inte fullt ut anses uppfylla de krav som ställs i dataskyddsdirektivet. Även i den generella lagen för myndighetsområdet behövs det alltså särskilda bestämmelser om rättelse av oriktiga personuppgifter.

Bestämmelser som syftar till personuppgifter ska korrigeras i andra fall

Förvaltningslagen innehåller också en bestämmelse som innebär att en myndighet ska ändra ett beslut som befunnits uppenbart oriktigt p.g.a. nya omständigheter eller av någon annan anledning (27 §). Det handlar då alltså inte om att rätta en felaktig uppgift, utan vad saken gäller är att ersätta ett beslut med ett nytt beslut. Till skillnad för vad som gäller i fråga om rättelse, innebär denna bestämmelse en skyldighet för myndigheten att fatta ett nytt beslut om de förutsättningar som anges i lagen är för handen.

Artikel 12 b i dataskyddsdirektivet innebär också en skyldighet att korrigera personuppgifter även i andra fall än då det är fråga om personuppgifter som är felaktiga i något avseende. Denna skyldighet har i svensk rätt också genomförts genom 28 § PuL, som föreskriver en skyldighet att rätta, blockera eller utplåna personuppgifter som över huvud taget har behandlats i strid med lagen eller anslutande föreskrifter. Denna skyldighet får uppfattas ha ett helt annat fokus än 27 § FL. Den sistnämnda bestämmelsen syftar till

att ett beslut som av någon anledning har blivit uppenbart oriktigt ska ersättas med ett nytt beslut. Fokus ligger alltså på om beslutet som sådant framstår som oriktigt av något skäl, inte på vilken kvalitet enskilda uppgifter har. Bestämmelsen är också, i likhet med 26 §, endast tillämplig i fråga om beslut och inte om myndigheters hantering av uppgifter i övrigt. Redan av detta skäl kan det konstateras att myndigheters skyldighet att ändra sina beslut enligt 27 § FL inte kan anses tillräcklig för att uppfylla dataskyddsdirektivets krav.

Vi kommer nedan att behandla frågan om personuppgiftslagens bestämmelser i fråga om rättelse av oriktiga uppgifter och korrigering av otillåtna behandlingar bör gälla också fortsättningsvis på myndighetsområdet eller ersättas med nya bestämmelser i den generella lagen. I samband med att vi behandlar frågan om hur myndigheternas skyldigheter i dessa avseenden bör regleras framöver tar vi också upp vad som bör gälla i fråga om skyldighet att underrätta tredje man om vidtagna rättelser.

15.4.2 En åtskillnad bör göras mellan korrigering i form av rättelse av felaktiga personuppgifter och korrigering när uppgifter har behandlats på ett otillåtet sätt

Bedömning: I den nya lagen bör det föras in dels en bestämmelse som tar sikte på en myndighets skyldighet att rätta felaktiga eller ofullständiga uppgifter, dels en bestämmelse som tar sikte på skyldigheten att korrigera en behandling som av andra skäl inte är tillåten enligt lagen.

Den personuppgiftsansvariges skyldighet att på begäran av den registrerade rätta felaktiga eller ofullständiga uppgifter samt att i övrigt rätta, blockera eller utplåna personuppgifter som har behandlats på ett otillåtet sätt regleras i en och samma bestämmelse både i dataskyddsdirektivet och i personuppgiftslagen (artikel 12.1 punkt b i direktivet respektive 28 § PuL). I förslaget till uppgiftsskyddsförordning har däremot gjorts en åtskillnad mellan å ena sidan skyldigheten att rätta felaktiga eller ofullständiga uppgifter (artikel 16) och å andra sidan skyldigheten att radera personuppgifter som av diverse andra skäl inte längre får behandlas (artikel 17).

Det kan konstateras att skyldigheten att rätta felaktiga eller ofullständiga personuppgifter har en direkt anknytning till det grundläggande kravet på den personuppgiftsansvarige att personuppgifter som behandlas ska vara riktiga och, om nödvändigt, aktuella samt att alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga eller ofullständiga korrigeras (artikel 6.1 punkt d i dataskyddsdirektivet och 9 § första stycket punkterna g och h PuL). Skyldigheten att i övrigt korrigera en otillåten behandling hänför sig inte mer specifikt till de krav som allmänt gäller i fråga om behandling av personuppgifter.

För den personuppgiftsansvarige torde det vara mer okomplicerat att bedöma om en personuppgift är felaktig eller ofullständig än om den registrerade exempelvis gör gällande att en personuppgift inte är relevant i förhållande till det ändamål för vilken uppgiften samlats in. Rimligen finns det inte heller något intresse för en personuppgiftsansvarig myndighet att behandla en personuppgift som är felaktig eller ofullständig. Rätten att få felaktiga eller ofullständiga personuppgifter korrigerade kan därför göras mer ovillkorlig än rätten att få personuppgifter som av andra skäl behandlas på ett otillåtet sätt korrigerade genom exempelvis utplåning. Följaktligen har, som redovisats ovan, i förvaltningslagen och processrättsliga regelverk införts en i princip ovillkorlig möjlighet för myndigheter och domstolar att rätta felaktiga uppgifter även i beslut.

Den nu redovisade skillnaden mellan grunderna för att få till stånd en korrigering av en behandling som är otillåten har emellertid inte kommit till något klart uttryck i dataskyddsdirektivet och personuppgiftslagen. Däremot görs alltså en tydlig åtskillnad i förslaget till uppgiftsskyddsförordning. Enligt vår uppfattning skulle en sådan åtskillnad leda till en avsevärt förbättrad tydlighet på myndighetsområdet när det gäller vilka krav som ställs på den personuppgiftsansvarige beträffande vilka åtgärder som ska vidtas när personuppgifter av olika skäl behandlas på ett otillåtet sätt. Till saken hör att även lagstiftaren på vissa områden uppmärksammat att 28 § PuL i vissa fall inte har ansetts utgjort en tydlig vägledning i fråga om vad som ska gälla. Det har därför i fråga om exempelvis Kronofogdemyndighetens register införts förtydligande bestämmelser i den registerförfattning som gäller för myndigheten och i fråga om vissa register har det föreskrivits att 28 § PuL inte alls ska

tillämpas utan i stället 26 § FL. I lagen (2011:1200) om elcertifikat har det vidare införts en särskild bestämmelse om rättelse som ersätter 28 § PuL och utgör en begränsning i skyldigheten att rätta i förhållande till vad som följer av den sistnämnda bestämmelsen.

Vi föreslår därför att det i den nya lagen införs dels en bestämmelse som tar sikte på en personuppgiftansvarig myndighets skyldighet att rätta felaktiga eller ofullständiga uppgifter, dels en bestämmelse som tar sikte på skyldigheten att korrigera en behandling som av andra skäl inte är tillåten enligt lagen. Nedan redovisas våra överväganden när det gäller utformningen av de båda bestämmelserna.

15.4.3 En särskild bestämmelse om skyldighet att rätta felaktiga eller ofullständiga personuppgifter

Förslag och bedömning: I den nya lagen införs en skyldighet för en myndighet att på begäran av den registrerade rätta eller komplettera en personuppgift som rör den registrerade, om uppgiften är felaktig eller ofullständig till följd av en åtgärd som inte har sin grund i myndighetens eller någon annans bedömning.

Någon särskild skyldighet att underrätta tredje man om en rättelse eller komplettering behöver inte införas.

Skyldighet att rätta

I den nya lagen bör en bestämmelse införas som föreskriver en skyldighet för en myndighet att på begäran av den registrerade rätta eller komplettera en personuppgift som rör den registrerade, om uppgiften är felaktig eller ofullständig till följd av en åtgärd som inte har sin grund i myndighetens eller någon annans bedömning. En sådan bestämmelse uppfyller de krav som ställs enligt både dataskyddsdirektivet och förslaget till uppgiftsskyddsförordning.

Genom bestämmelsen uttrycks både en rätt för den registrerade att begära rättelse eller komplettering och en skyldighet för myndigheten att korrigera en personuppgift om den är felaktig eller ofullständig. Att detta uttrycks i bestämmelsen utgör, mot bakgrund av dataskyddsdirektivets krav, en nödvändig komplettering

av myndigheters befogenhet att rätta oriktiga uppgifter enligt 26 § FL. En sådan bestämmelse gör det också tydligt att skyldigheten att rätta inte enbart gäller felaktiga uppgifter i beslut, utan gäller i fråga om alla former av dokumentation där personuppgifter förekommer.

I materiellt hänseende avses skyldigheten att rätta en felaktig eller komplettera en ofullständig personuppgift inte i någon nämnvärd utsträckning skilja sig från den befogenhet för en myndighet som följer av förvaltningslagen. Det ska alltså vara frågan om ett fel eller en ofullständighet som har uppstått på grund av en åtgärd som inte har sin grund i myndighetens eller någon annans bedömning. Det kan alltså handla om sådana förbiseendefel som omfattas av 26 § FL eller exempelvis ett fel som uppstått p.g.a. något tekniskt förfarande. Inom ramen för denna bestämmelse ska det alltså inte finnas utrymme för att korrigera en personuppgift som ur ett objektivt perspektiv är riktig, men som den registrerade av något skäl anser är felaktig eller ofullständig i förhållande till ändamålet med behandlingen. I det fallet handlar det ju inte om att en uppgift är felaktig eller ofullständig utifrån direktivets krav på att uppgifter som behandlas ska vara riktiga. I stället behöver det göras en bedömning av om uppgiften är adekvat eller relevant med hänsyn till ändamålet med den aktuella behandlingen. Den typen av bedömningar hör i stället samman med den bestämmelse som vi föreslår nedan. För att det ska vara frågan om en rättelse eller komplettering i den mening som nu avses ska den felaktiga uppgiften kunna ersättas av en annan uppgift som är riktig eller kompletteras med en uppgift så att den blir fullständig i en objektiv mening, exempelvis om ett namn är felaktigt eller om endast delar av ett namn har återgetts i en handling hos myndigheten.

I 26 § FL, liksom i de processrättsliga reglerna som är utformade på motsvarande sätt, sägs att det ska vara fråga om en ”uppenbar oriktighet” som har orsakats av ”skrivfel, räknefel eller annat liknande förbiseende”. En felaktighet eller ofullständighet på grund av en åtgärd som inte har sin grund i någons bedömning kan dock per definition uppfattas vara uppenbar till sin natur. Kravet att oriktigheten ska vara uppenbar kan dock anses medföra att en viss ytterligare utredningsskyldighet åligger den som påkallar en rättelse enligt förvaltningslagens bestämmelse. Mot den bakgrunden bör något sådant krav inte ställas upp. Men även om ett sådant krav inte tas in

i den bestämmelse som vi nu föreslår, torde enligt vår mening detta knappast innebära någon större skillnad i sak. Det kan sägas ligga i sakens natur att om en felaktighet av nu aktuellt slag kan konstateras föreligga, så är felaktigheten uppenbar. Den bestämmelse som vi nu föreslår innebär därför enligt vår uppfattning i detta hänseende inte någon nämnvärd skillnad i förhållande till den möjlighet som förvaltningslagen ger myndigheter att rätta oriktiga uppgifter.

Genom att det införs en särskild bestämmelse i den nya lagen om en skyldighet att rätta eller komplettera en felaktig eller ofullständig personuppgift, som åtskiljs från en myndighets skyldighet att korrigera behandlingar som är otillåtna i andra avseenden, uppnås enligt vår mening en ökad tydlighet. En sådan bestämmelse stämmer också bättre överens med de övriga regelverk som rör myndigheters hantering av uppgifter. Inom ramen för de krav som följer av dataskyddsdirektivet åstadkommer man på så sätt en reglering som så nära som möjligt ansluter till förvaltningslagens och de processrättsliga regelverkens bestämmelser om rättelse. Dessa bestämmelser avses ge uttryck för en rimlig balans mellan intressen som rör å ena sidan att de uppgifter som en myndighet hanterar bör vara korrekta och å andra sidan att ett beslut som är slutgiltigt avfattat inte ska kunna ändras på ett godtyckligt sätt.

Några särskilda regler om en myndighets skyldighet att dokumentera att en rättelse av en felaktig eller ofullständig personuppgift har skett behöver inte införas. I stället gäller vad som följer av andra regler (se t.ex. 32 § tredje stycket andra meningen FPL).

Underrättelse till tredje man om en rättelse

Enligt artikel 12 c i dataskyddsdirektivet ska den registrerade ha rätt att få ”genomfört” att tredje man, som fått del av en felaktig eller ofullständig personuppgift, underrättas om varje rättelse som utförts enligt artikel 12 b. En sådan skyldighet finns dock inte om det visar sig vara omöjligt eller innebära en oproportionerligt stor ansträngning.

Vi vill inledningsvis framhålla att det inte kan anses följa av direktivets krav att det skulle finnas en underrättelseskyldighet enligt artikel 12 c i förhållande till varje tredje man som tagit del av

uppgifter i ett offentligt register eller fått del av personuppgifter genom rätten att ta del av allmänna handlingar. En sådan skyldighet skulle rimligen vara omöjlig att uppfylla eller innebära en oproportionerligt stor ansträngning. I en myndighets verksamhet torde underrättelseskyldigheten i förhållande till tredje man därför i första hand bli aktuell beträffande en annan part som figurerar i eller direkt berörs av samma ärende som den registrerade.

Enligt 26 § förvaltningslagen är tredje mans intresse tillvarataget på så sätt att den som är part ska ges tillfälle att yttra sig innan rättelse sker, om ärendet avser myndighetsutövning mot någon enskild och åtgärden inte är obehövlig. Eftersom befogenheten att rätta enligt denna bestämmelse är begränsad till en myndighets beslut, gäller alltså skyldigheten att ge part tillfälle att yttra sig också enbart när rättelse avses ske i ett beslut. Det förefaller främmande att det skulle finnas en skyldighet att låta part yttra sig över en sådan sak innan myndigheten har fattat sitt beslut. Fram till denna tidpunkt förfogar ju parterna i princip över de uppgifter som genom dem själva tillförts ärendet. Av såväl förvaltningslagen som de processrättsliga regelverken följer däremot att en myndighet eller domstol under ett pågående mål eller ärende har en skyldighet att låta part ta del av vad som tillförts ärendet eller målet. Därigenom sker alltså en underrättelse av om uppgifter har ändrats som rör någon av parterna. Dessutom följer av 21 § FL att part ska underrättas om det beslut som ersätter det rättade beslutet. Motsvarande skyldigheter följer även av de processrättsliga regelverken.

Enligt vår uppfattning bör det inte föras in någon bestämmelse i den nya lagen som ger den registrerade en särskild rätt att påkalla underrättelse till tredje man då en rättelse eller komplettering har skett. Det får anses tillräckligt med de skyldigheter som myndigheten ändå har enligt övriga regelverk att låta parter ta del av vad som tillförts ett ärende och att höra part innan rättelse görs i ett beslut. Enbart den omständigheten att det i så fall inte blir fråga om en åtgärd som den registrerade förfogar över på det sätt som är fallet enligt artikel 12 c i dataskyddsdirektivet innebär enligt vår mening inte att direktivets krav inte är uppfyllda i detta avseende. Vi anser alltså att det är förenligt med dataskyddsdirektivets bestämmelser att inte föreslå att det av den nya lagen ska följa någon särskild rätt för den registrerade att begära att en myndighet underrättar tredje man om en rättelse eller komplettering.

15.4.4 En särskild bestämmelse om skyldighet att korrigera en behandling som är otillåten

Förslag och bedömning: En bestämmelse införs som föreskriver att en personuppgift på begäran av den registrerade ska avskiljas från fortsatt behandling och inte lämnas ut till en enskild annat än med stöd av 2 kap. TF eller utplånas, om uppgiften rör honom eller henne och inte får behandlas enligt den nya lagen eller föreskrifter som har meddelats med stöd av den.

Rätten att begära korrigering i form av avskiljande från fortsatt behandling och hinder mot spridning eller genom utplåning ska inte gälla personuppgifter i en myndighets beslut.

En allmän skyldighet att korrigera

Enligt artikel 12 b i dataskyddsdirektivet ska medlemsstaterna säkerställa att varje registrerad får personuppgifter rättade, utplånade eller blockerade som inte behandlas i enlighet med bestämmelserna i direktivet även i andra fall än då uppgifterna är ofullständiga eller felaktiga. Denna skyldighet tar ospecificerat sikte på alla krav som uppställs i direktivet för att en behandling ska vara tillåten. Det kan alltså handla om personuppgifter som varken är felaktiga eller ofullständiga, dvs. personuppgifter som i och för sig är riktiga, men ändå inte får behandlas enligt direktivet på grund av att de exempelvis är för gamla eller inte relevanta.

Den generella lagen bör därför innehålla en bestämmelse som ger registrerade rätt att, förutom att åberopa att en rättelse eller komplettering bör ske, göra gällande att en personuppgift inte får behandlas av myndigheten i fråga. Av bestämmelsen bör också framgå att myndigheten är skyldig att korrigera en behandling om den är otillåten. Frågan om en personuppgift behandlas i strid med den nya lagen får bedömas mot bakgrund av de bestämmelser som är tillämpliga på behandlingen och för det ändamål som myndigheten behandlar uppgiften (jfr RÅ 2006 ref. 86).

Vilka korrigeringsåtgärder ska vidtas?

I såväl dataskyddsdirektivet som personuppgiftslagen används begreppen att rätta, blockera eller utplåna för att beskriva de former av korrigering som ska göras för att en behandling av personuppgifter ska bli tillåten. Enligt vår mening bör alltså begreppet rättelse förbehållas de fall då en myndighet korrigerar en personuppgift som är felaktig till sitt innehåll. Den skyldighet som vi nu talar om, dvs. att myndigheten ska korrigera en behandling av personuppgifter som inte är förenlig med gällande bestämmelser, måste alltså benämnas på annat sätt än genom termen rättelse.

I såväl dataskyddsdirektivet och personuppgiftslagen används begreppen blockera eller utplåna en personuppgift för att beskriva de åtgärder som ska vidtas. Vilken metod som ska användas har det i princip ansetts vara upp till den personansvarige att avgöra, även när den ansvarige är en myndighet (se t.ex. prop. 2007/08:116 s. 20 om rättelse i Kronofogdemyndighetens databaser).

Utplåning

Eftersom utplåning anses innebära att personuppgifter tas bort från informationssamlingarna på ett sådant sätt att de inte ur dessa samlingar kan återskapas, bör en sådan åtgärd vidtas av en myndighet bara om den är förenlig med huvudprincipen att allmänna handlingar ska bevaras i myndigheternas arkiv. Detta innebär att utplåning av personuppgifter i allmänna handlingar som utgör s.k. färdiga elektroniska handlingar, handlingar i pappersform och sådana handlingar som tagits om hand för arkivering inte bör ske utan uttryckligt lagstöd. Sådant stöd torde finnas endast i absoluta undantagsfall. Som exempel kan nämnas att det i 7 kap. 2 § andra stycket patientdatalagen (2008:355) finns bestämmelser om att personuppgifter ska utplånas ur kvalitetsregister om den enskilde motsätter sig att de behandlas. Enligt 8 kap. 4 § samma lag får Inspektionen får vård och omsorg på ansökan av en patient eller någon annan som omnämns i en patientjournal besluta att journalen helt eller delvis ska förstöras. Den bestämmelse som vi nu föreslår bör alltså inte kunna åberopas till stöd för en myndighet att utplåna personuppgifter i allmänna handlingar utan en bedömning att en

sådan åtgärd är förenlig med de intressen som bär upp regler om arkiv.

Såvitt avser personuppgifter i allmänna handlingar torde således utrymmet för myndigheter att utplåna personuppgifter som har behandlats på ett sätt som inte är förenligt med gällande bestämmelser vara mycket litet. Frågan är vilken åtgärd myndigheten i stället ska vidta för att korrigera en behandling som kommer till uttryck eller dokumenteras på det sättet fast den inte är tillåten.

Gallring

Frågan om personuppgifter har behandlats under alltför lång tid bedöms på myndighetsområdet utifrån vad som föreskrivs i bestämmelser om gallring. Den åtgärd som ska vidtas i så fall är alltså att följa tillämplig gallringsbestämmelse. Någon särskild bestämmelse om detta behöver därför inte föras in i den nya lagen (se vidare kapitel 14).

Blockering ersätts med en åtgärd som innebär att personuppgifter avskiljs från fortsatt behandling

I den händelse en myndighet har behandlat personuppgifter som inte är adekvata eller relevanta utifrån ändamålet med den aktuella behandlingen är emellertid frågan om vilken åtgärd som bör vidtas. När det gäller det s.k. Kringresanderegistret hos Polismyndigheten i Skåne, som befunnits olagligt i flera avseenden (se avsnitt 18.1) har åtgärder vidtagits som inneburit att uppgiftssamlingen har avslutats och gallrats (Säkerhets- och integritetsskyddsnämndens uttalande den 11 december 2014, dnr 463-2013). Två kopior av uppgiftssamlingen har dock sparats för att kunna besvara frågor om förekomst.

Den åtgärd som dataskyddsdirektivet och personuppgiftslagen anvisar som alternativ åtgärd till utplåning för att korrigera en otillåten behandling är att blockera personuppgifterna. I 3 § PuL definieras blockering som en åtgärd som vidtas för att personuppgifterna ska vara förknippade med information om att de är spärrade och om anledningen till spärren och för att uppgifterna inte ska lämnas ut till tredje man annat än med stöd av 2 kap. TF. Av

definitionen anses följa att de blockerade uppgifterna får användas internt hos den personuppgiftsansvarige och hos ett personuppgiftsbiträde under förutsättning att det framgår att de är blockerade och anledningen till den åtgärden. Däremot får uppgifterna inte lämnas ut till tredje man. Det anses vara upp till den personuppgiftsansvarige att bestämma hur det tekniskt ska åstadkommas att de blockerade uppgifterna är förknippade med information om blockeringen (Öman/Lindblom, s. 85).

Det är emellertid svårt att se framför sig på vilket sätt åtgärden blockering skulle fylla någon funktion från den registrerades perspektiv när det gäller en myndighets verksamhet. Såvitt avser hans eller hennes intresse av att myndigheten endast ska behandla personuppgifter som är adekvata, relevanta och nödvändiga för det ändamål som behandlingen sker förefaller åtgärder av den typ som har vidtagits i fråga om det s.k. Kringresanderegistret vara mer relevanta än att en blockering görs, oavsett vad det sistnämnda nu kan tänkas innebära. Det centrala i sammanhanget förefaller nämligen vara att myndigheten upphör med att behandla personuppgifter som inte får ingå i den aktuella behandlingen. Det kan exempelvis handla om att uppgifterna inte är relevanta utifrån syftet med ett visst register eller att känsliga personuppgifter behandlas trots att det inte finns någon tillämplig undantagsbestämmelse som tillåter det.

En åtgärd som innebär att myndigheten upphör med behandling av en personuppgift som inte är tillåten utifrån syftet med den aktuella behandlingen kan lämpligen beskrivas som att uppgiften avskiljs från fortsatt behandling. Genom begreppet avskiljs uttrycks att den aktuella personuppgiften i fortsättningen inte får ingå i den behandling som är i fråga. Samtidigt framgår att det inte är frågan om att i teknisk mening fullständigt gallra uppgiften eller att utplåna den, utan den kan och bör bevaras i enlighet med vad som i övrigt gäller för myndighetens verksamhet och är lämpligt i sammanhanget. Om och på vilket sätt personuppgiften bör bevaras hos myndigheten efter ett avskiljande får alltså bedömas med utgångspunkt i vilken verksamhet myndigheten bedriver och för vilka skäl ett fortsatt bevarande kan vara nödvändigt. I fråga om det s.k. Kringresanderegistret hade det exempelvis, med hänsyn till möjligheterna att ställa eventuella beslutsfattare till ansvar och att reglera krav på skadestånd, varit högst olämpligt att utplåna de personuppgifter

som ingick i registret liksom registret som sådant. Det kan vidare tilläggas att begreppet avskiljande i dataskyddsdirektivets perspektiv kan liknas vid att personuppgifterna blockeras eller spärras, i vart fall med avseende på den aktuella behandlingen hos myndigheten. I och med att uppgifter på detta sätt avskiljs från den aktuella behandlingen, saknas det vidare ett behov av att särskilt göra en markering av uppgiften att den är ”blockerad”.

Begreppet blockering innebär enligt legaldefinitionen i personuppgiftslagen att personuppgifterna inte ska lämnas ut till tredje man annat än med stöd av 2 kap TF. Den senare markeringen förefaller i och för sig överflödig, eftersom detta redan följer av att bestämmelserna i 2 kap. TF gäller före bestämmelserna i personuppgiftslagen (jfr 8 § PuL).

Någon motsvarande rätt att få uppgifter ur allmänna handlingar som finns beträffande själva handlingen finns inte. Om en myndighet inte vill lämna ut en uppgift ur en allmän handling, saknas möjlighet för den enskilde att överklaga beslutet (6 kap. 4 och 7 §§ OSL). Såvitt vi har erfarit finns det inga indikationer på att åtgärden ”blockering” skulle ha åberopats som skäl för att inte lämna ut en personuppgift till tredje man eller att bestämmelsen i personuppgiftslagen i detta avseende har lett till några problem på myndighetsområdet. Det förefaller vidare främmande att en myndighet självmant skulle ägna sig åt att sprida personuppgifter som av något skäl bör ”blockeras”. Å andra sidan finns inget tungt vägande skäl mot att en bestämmelse om rätt till korrigering av en otillåten behandling i en myndighets verksamhet även bör omfatta att uppgifterna i fråga inte får lämnas ut annat än med stöd av 2 kap. TF. En sådan rätt kan emellertid på myndighetsområdet bara avse utlämnande till enskilda och inte till en annan myndighet, eftersom myndigheter har en överklagbar rätt enligt 6 kap. 5 § OSL att begära ut både uppgifter och handlingar. I vilken utsträckning en myndighet ska vara skyldig att lämna ut en ”blockerad” personuppgift till en annan myndighet får därför avgöras utifrån de andra bestämmelser som gäller sådant uppgiftsutbyte.

Vi föreslår mot bakgrund av det anförda att begreppet blockering inte ska användas i den nya lagen utan ersättas av en åtgärd som avser att en myndighet, om en personuppgift inte får behandlas, ska avskilja uppgiften från fortsatt behandling och inte heller lämna ut en sådan uppgift till en enskild annat än med stöd av 2 kap. TF.

Avslutningsvis kan nämnas att enligt förslaget till uppgiftsskyddsförordning ska en otillåten behandling åtgärdas genom radering (artiklarna 17.1–17.3) eller att behandlingen av personuppgifter begränsas (artiklarna 17.4). Enligt vår bedömning ryms den bestämmelse som vi nu föreslår även inom de krav som förordningen föreslås uppställa i denna del.

Undantag för en myndighets beslut

Enligt 1 kap. 9 § RF ska domstolar och myndigheter i sin verksamhet beakta allas likhet inför lagen samt iaktta saklighet och opartiskhet.

Detta grundlagsstadgade krav innebär att t.ex. att domstolar och myndigheter ska utforma sina beslut så att de även betraktade utifrån framstår som sakliga och opartiska. Redan genom detta grundläggande krav på myndigheternas verksamhet, oavsett i vilken form den tar sig uttryck, finns en starkt styrande kraft som verkar för att domstolars och myndigheters beslut ska hålla hög kvalitet i så måtto att de inte innehåller andra uppgifter än sådana som är korrekta och relevanta för den fråga som avgjorts genom beslutet.

I förvaltningslagen samt i de processrättsliga regelverken finns kompletterande bestämmelser som styr hur myndigheters och domstolars beslut ska vara utformade. Ett gemensamt krav är bl.a. att det av ett beslut ska framgå de skäl som bestämt utgången i ärendet eller målet. Av dessa bestämmelser, liksom av de grundläggande bestämmelserna i 9 § PuL, följer att en omständighet som anges i ett beslut ska vara adekvat, relevant och påkallad för att motivera utgången i ärendet eller målet. Det innebär i sin tur att de krav som ställs i 9 § PuL måste bedömas med beaktande av de legitima och grundläggande värden och intressen som ligger till grund för en domstols eller förvaltningsmyndighets verksamhet (jfr RH 2008:87). Vad gäller en sådan verksamhet ligger det i sakens natur att det i allmänhet måste finnas ett relativt stort utrymme för myndigheten eller domstolen att själv avgöra vilka omständigheter som bör återges i en handling där domstolens eller myndighetens ställningstagande beträffande ett visst mål eller ärende redovisas.

Av andra regelverk som styr hur myndigheter och domstolar ska utforma sina beslut finns alltså redan högt ställda krav som

motsvarar de grundläggande krav som gäller för behandling av personuppgifter i dataskyddsdirektivet.

Enligt förvaltningslagen och processrättsliga regelverk finns vidare uttryckliga bestämmelser om möjlighet att få beslut omprövade av den beslutande instansen eller, efter ett överklagande, av en högre instans. Det finns också särskilda regler om omprövning som gäller i viss myndighetsverksamhet. Det finns därutöver möjlighet att på extraordinär väg föra talan om ändring genom s.k. resning. Av allmänna rättsgrundsatser följer också ytterligare möjligheter för myndigheter att ompröva sina beslut.

Både en omprövning av ett beslut av beslutinstansen eller en ändring efter ett överklagande syftar till att ändra ett besluts rättsverkningar, dvs. att själva beslutet ska ändras. En förutsättning för att det ska finnas en rätt att överklaga ett beslut är således enligt 22 § FL att beslutet har gått den klagande emot. Det innebär att om en persons klagomål rörande ett beslut inte går ut på att själva beslutet ska ändras eller upphävas utan enbart avser beslutsmotiveringen, finns det ingen klagorätt (se t.ex. RÅ 2006 ref. 21).

Genom JO och JK:s verksamhet kan den enskilde däremot få prövat om en myndighet eller domstol, eller en enskild tjänsteman som är anställd där, förtjänar kritik för att ett beslut inte har utformats i överensstämmelse med gällande regelverk, exempelvis genom att i motiveringen ta med omständigheter som inte är relevanta för att avgöra den fråga som är aktuell i målet eller ärendet (se t.ex. JO:s beslut den 21 mars 2012, dnr 511-2011, angående hur en tingsrätts dom hade formulerats). Ett sådant ärende kan vidare i sin tur leda till, om det är fråga om ett tillräckligt klandervärt beteende, att beslutsfattaren blir föremål för disciplinåtgärd eller att det väcks åtal för brottet tjänstefel. Grava felbedömningar som kommit till uttryck i ett beslut kan också ge utrymme för att utkräva ett skadeståndsrättsligt ansvar enligt 3 kap. 2 § skadeståndslagen (1972:207) på grund av fel eller försummelse från statens eller en kommuns sida (se t.ex. NJA 2003 s. 285).

Om ett beslut har utformats på ett så klandervärt sätt att beslutsfattaren i fråga gör sig skyldig till brott, kan en person som har orsakats lidande på grund av det undermåligt utformade beslutet få skadestånd enligt de allmänna bestämmelserna i skadeståndslagen. I de fall ett beslut har ändrats till följd av att en person har begärt omprövning av det eller överklagat detsamma kan det

vidare också uppstå en situation där en rätt till skadestånd enligt 48 § PuL kan föreligga. Genom det ändrade beslutet kan en personuppgift, som tidigare ansetts riktig, nu anses felaktig. En felaktig personuppgift har alltså behandlats, vilket beroende på omständigheterna kan ha ställt till med både ekonomisk skada och lidande för den enskilde. Myndigheten kan då i egenskap av personuppgiftsansvarig bli skadeståndsskyldig för att den, som det sedermera visat sig, har behandlat en felaktig personuppgift (se t.ex. JK:s beslut den 2 mars 2011, dnr 8156-09-40).

Sammanfattningsvis kan det konstateras att det, vid sidan av vad som sägs i 9 § PuL, finns regler som ställer krav på vilken kvalitet som personuppgifter ska hålla som behandlas i myndigheters och domstolars beslut. Det finns också ett förvaltningsrättsligt och processrättsligt regelverk som i princip uttömmande reglerar i vilken utsträckning ett beslut av en myndighet eller domstol kan ändras. Detta regelverk har utformats med avseende på att både ta hänsyn till parters intresse av att kunna få beslut ändrade och intresset av att man ska kunna utgå från att ett beslut, varigenom ett ärende eller mål har avgjorts, står fast och inte utan vidare kan ändras. Det finns också inom ramen för den ordning som beskrivits ovan möjlighet att få prövat om utformningen av ett avgörande från en myndighet eller domstol inte uppfyller de krav som ställs. Det är vidare möjligt att göra anspråk på rätt till skadestånd.

Enligt vår uppfattning saknas det mot denna bakgrund ett behov av att i den nya lagen tillhandahålla ytterligare en möjlighet för den registrerade att föra talan om att ett beslut av en myndighet eller en domstol inte har utformats på ett sätt som motsvarar de krav som gäller för beslutsfattandet. Vi anser också att det från principiella utgångspunkter framstår som tveksamt att tillhandahålla en sådan rätt vid sidan av den ordning som finns att tillgå genom andra regelverk, vilka har funnits under lång tid och har sin grund i de allmänna rättsgrundsatser som bär upp de förvaltningsrättsliga och processrättsliga regelverken. Ett sådant ställningstagande är enligt vår uppfattning väl förenligt med de möjligheter till undantag från skyldigheterna i artikel 12 b i dataskyddsdirektivet som föreskrivs i artikel 13.1 beträffande skyddet för andras fri- och rättigheter. Detsamma gäller undantagen i förslaget i uppgiftsskyddsförordningen från skyldigheten att radera, jfr artikel 17.3 d.

Rätten att begära korrigering i form av avskiljande från fortsatt behandling och hinder mot spridning eller genom utplåning av en personuppgift ska alltså inte gälla uppgifter i en myndighets beslut. Däremot har den registrerade rätt att enligt den bestämmelse om rättelse som vi föreslagit ovan begära att ett beslut rättas om det innehåller en personuppgift som är felaktig eller ofullständig.

Skyldighet att underrätta tredje man

Vi har ovan redovisat vår uppfattning att det inte behöver införas någon särskild skyldighet att underrätta tredje man om att en rättelse skett i pågående ärenden eller mål, eftersom det är tillräckligt med den skyldighet att kommunicera som redan åligger myndigheter och domstolar. När det gäller skyldigheten att korrigera en otillåten behandling, som enligt vårt förslag enbart gäller behandlingar som inte har samband med utformning av ett beslut, gör vi samma bedömning. När en personuppgift avskiljs från fortsatt behandling eller undantagsvis utplånas bedömer vi alltså att det är tillräckligt med en myndighets skyldighet att kommunicera som redan finns enligt andra regelverk för att uppfylla direktivets krav i detta hänseende.

16 Anmälan till tillsynsmyndigheten m.m.

16.1 Allmänna dataskyddsrättsliga regler

Dataskyddsdirektivet

Anmälningsskyldighet

Direktivet bygger på huvudregeln att all helt eller delvis automatiserad behandling av personuppgifter ska anmälas till tillsynsmyndigheter, artikel 18.1. Denna huvudregel om anmälningsplikt måste medlemsstaterna föreskriva. I punkten 48 i ingressen till direktivet anges att anmälningsförfarandet är avsett att göra behandlingens ändamål och viktigaste egenskaper allmänt kända för att säkerställa att behandlingen sker i enlighet med de nationella åtgärder som vidtas för att genomföra direktivet.

Medlemsstaterna ska, enligt artikel 19.1, precisera vilka uppgifter som anmälan ska innehålla, dock ska den innehålla åtminstone följande uppgifter.

a) Den registeransvariges eller dennes eventuella företrädares namn och adress.

b) Ändamålen med behandlingen.

c) En beskrivning av den eller de kategorier av registrerade som berörs och av de uppgifter eller kategorier av uppgifter som hänför sig till berörda registrerade.

d) Mottagarna eller de kategorier av mottagare till vilka uppgifterna kan komma att lämnas ut.

e) Föreslagna överföringar av uppgifter till tredjeland.

f) En allmän beskrivning som gör det möjligt att preliminärt bedöma lämpligheten av vidtagna säkerhetsåtgärder enligt artikel 17.

Medlemsstaterna ska vidare, enligt artikel 21.2, föreskriva att tillsynsmyndigheten ska föra ett allmänt tillgängligt register över anmälda behandlingar. Registret ska åtminstone innehålla de uppgifter som anges i artikel 19.1 a–e och vara allmänt tillgängligt.

Undantag från anmälningsplikten

Anmälningsplikten enligt artikel 18.1 är en huvudregel som medlemsstaterna inom vissa gränser får föreskriva undantag från. Möjliga undantag anges i artikel 18.2–4. Alternativt kan medlemsstaterna meddela föreskrifter om ett förenklat anmälningsförfarande.

Av intresse för myndigheters behandlingar av personuppgifter är till en början artikel 18.2 som anger två undantagsmöjligheter.

Den första gäller de typer av behandlingar i samband med vilka det med hänsyn till de behandlade uppgifterna inte är sannolikt att de registrerades fri- och rättigheter kränks. För att undantag ska få göras krävs dock att det för dessa typer av behandling anges behandlingens ändamål, vilka uppgifter eller kategorier av uppgifter som behandlas, vilka registrerade eller kategorier av registrerade som avses, till vilka mottagare eller kategorier av mottagare uppgifterna lämnas ut och hur länge uppgifterna ska bevaras.

Den andra möjligheten till undantag gäller när den registeransvarige, i enlighet med den nationella lagstiftning som gäller för honom eller henne, har utsett ett uppgiftsskyddsombud. Uppgiftsskyddsombudet ska ha till uppgift att dels på ett oberoende sätt säkerställa den interna tillämpningen av de nationella bestämmelser som har antagits till följd av direktivet, dels föra ett register över de behandlingar som utförs av den registeransvarige. Registret ska innehålla de obligatoriska uppgifter som en anmälan skulle ha innehållit med undantag för beskrivning av de säkerhetsåtgärder som har vidtagits, dvs. registret ska innehålla de uppgifter som anges i artikel 19.1 a–e. Uppgiftsskyddsombudet ska på detta sätt säkerställa att de registrerades fri- och rättigheter sannolikt inte kommer att kränkas som en följd av behandlingarna. Ombudet ska vidare rådfråga tillsynsmyndigheten i tveksamma fall rörande huruvida det krävs en förhands-

kontroll av särskilt riskfyllda behandlingar (artikel 20.2). I punkt 49 i ingressen betonas att den person som utses till uppgiftsskyddsombud måste – vare sig han eller hon är anställd av den registeransvarige eller inte – ha möjlighet att utöva sin verksamhet på ett fullständigt oberoende sätt.

I artikel 18.3 ges en tredje möjlighet för medlemsstaterna att föreskriva undantag, nämligen för behandling i författningsreglerade register vars enda syfte är att förse allmänheten med information och som är tillgängliga antingen för allmänheten eller för var och en som kan styrka ett berättigat intresse.

Förhandskontroll

Enligt artikel 20 måste vissa särskilt riskfyllda behandlingar anmälas och kontrolleras innan de påbörjas. Till skillnad från den ordinarie anmälningsskyldigheten enligt artikel 18.1 ska alltså tillsynsmyndigheten göra en kontroll i det särskilda fallet. Det är dock medlemsstaterna som ska bestämma vilka behandlingar som kan innebära särskilda risker för den registrerades fri- och rättigheter och därför kräver förhandskontroll (artikel 20.1). I punkt 53 i ingressen anförs att vissa typer av behandling på grund av sin natur, sin omfattning eller sitt ändamål kan innebära särskilda risker för att de registrerades fri- och rättigheter kränks. Som exempel anges behandling som har till ändamål att utesluta den berörde från möjligheten att utöva en rättighet, ta emot en förmån eller ingå ett avtal och sådan behandling som innebär användning av ny teknik. Förhandskontroller ska utföras av tillsynsmyndigheten efter anmälan (artikel 20.2). Kontrollen kan alternativt ske som ett led i det nationella parlamentets förberedande arbete med en åtgärd eller som ett led i arbetet med en åtgärd som grundas på en sådan lagstiftande åtgärd som definierar behandlingens art och anger lämpliga skyddsåtgärder (artikel 20.3). Från bestämmelserna i artikel 20 om förhandskontroll föreskrivs inga särskilda undantag.

Behandlingarnas offentlighet

Även för de fall där medlemsstaterna utnyttjat möjligheten att föreskriva om undantag från huvudregeln om anmälningsplikt, har medlemsstaterna ett fortsatt ansvar för att se till att behandlingarna görs offentligt tillgängliga. Den som vill ska kunna få uppgifter om en behandling även om den inte har anmälts till tillsynsmyndigheten. Detta följer av artikel 21.1 och 3. Medlemsstaterna får dock föreskriva att detta inte ska gälla för sådana författningsreglerade register som undantagits från anmälningsplikt enligt artikel 18.3.

Härutöver gäller att medlemsstaterna får föreskriva begränsningar i kraven i artikel 21 på behandlingars offentlighet med stöd av artikel 13.1, dvs. då en begränsning är en nödvändig åtgärd med hänsyn till något av de skäl som anges i punkt a–g, t.ex. med hänvisning till skyddet av den registrerades eller andras fri- och rättigheter. Begränsningar kan alltså komma i fråga för såväl tillsynsmyndighetens register över anmälda behandlingar som registeransvarigas ansvar att tillhandahålla allmänheten information.

Personuppgiftslagen

Dataskyddsdirektivets bestämmelser om anmälan till tillsynsmyndigheten m.m. har genomförts i Sverige genom 36–42 §§ PuL och kompletterande bestämmelser i personuppgiftsförordningen samt Datainspektionens föreskrifter. I personuppgiftslagens förarbeten uttalades att det på grund av artikel 18.1 i direktivet var nödvändigt att föreskriva att alla automatiserade behandlingar ska anmälas till tillsynsmyndigheten. Dock ansågs att tillsynsmyndighetens verksamhet, dvs. Datainspektionens, borde koncentreras till att ge råd och sprida kunskap om de materiella reglerna och att utöva tillsyn över att reglerna följs. Det var därför viktigt att fullt ut utnyttja de möjligheter till undantag från anmälningsskyldigheten som direktivet medger. På det sättet borde anmälningsskyldigheten kunna begränsas till ett minimum (prop. 1997/98:44 s. 98).

Anmälningsskyldighet

Huvudregeln om anmälningsskyldighet för helt eller delvis automatiserad behandling slås fast i 36 § första stycket PuL. Anmälan till tillsynsmyndigheten ska göras av den personuppgiftsansvarige innan behandlingen eller en serie av sådana behandlingar med samma ändamål genomförs. Tillsynsmyndigheten gör ingen prövning av behandlingens lagenlighet eller liknande med anledning av en anmälan utan för in uppgifter om behandlingen i ett automatiserat register över anmälda personuppgiftsbehandlingar som inspektionen för enligt 7 § PuF. Vidare ska personuppgiftsansvariga som utser eller entledigar ett personuppgiftsombud anmäla detta till tillsynsmyndigheten (36 § andra stycket PuL).

Genom 16 § 6 PuF har Datainspektionen bemyndigats att meddela föreskrifter om vad en anmälan ska innehålla. Enligt 6 § DIFS 2013:1 ska anmälan innehålla motsvarande uppgifter som anges i artikel 19.1 i direktivet. Ändringar av något förhållande ska också anmälas.

Undantag från anmälningsskyldigheten

Från huvudregeln om anmälningsskyldighet finns flera undantag.

Enligt 36 § tredje stycket PuL får regeringen, eller den myndighet som regeringen bestämmer, meddela föreskrifter om undantag från anmälningsskyldigheten enligt första stycket för sådana typer av behandlingar som sannolikt inte kommer att leda till otillbörligt intrång i den personliga integriteten (jfr artikel 18.2 första strecksatsen). Så har skett genom 3–5 §§ PuF samt 3–5 §§ DIFS 2013:1 (se även 6 § PuF med bemyndigande för Datainspektionen att meddela undantag för behandlingar som avses i 36 § tredje stycket PuL). Enligt dessa gäller följande undantag från anmälningsskyldigheten såvitt är av intresse nu.

- Behandling av personuppgifter som utförs till följd av en myndighets skyldighet enligt 2 kap. TF att lämna ut allmän handling (3 § 1 PuF).
- Behandling av personuppgifter som till följd av arkivlagen (1990:782) eller arkivförordningen (1991:446) utförs av arkivmyndighet (3 § 2 PuF).

- Behandling av personuppgifter som regleras genom särskilda föreskrifter i lag eller förordning i andra fall än enligt 2 kap. TF eller arkivlagstiftningen (3 § 3 PuF).
- Behandling av personuppgifter i löpande text eller sådant ostrukturerat material som avses i 5 a § PuL (4 § PuF).
- Behandling av personuppgifter som sker efter samtycke från den registrerade (4 § DIFS 2013:1).
- Behandling av personuppgifter som har samlats in från den registrerade om behandlingen är nödvändig för att uppfylla bestämmelser i lag eller förordning under villkor att den personuppgiftsansvarige själv för en förteckning över behandlingarna med de uppgifter som annars skulle ha anmälts (5 § d DIFS 2013:1).
- Behandling av personuppgifter som får behandlas på hälso- och sjukvårdsområdet enligt 18 § PuL (känsliga personuppgifter) under villkor att den personuppgiftsansvarige själv för en förteckning över behandlingarna med de uppgifter som annars skulle ha anmälts (5 § e DIFS 2013:1).

Ett ytterligare undantag från anmälningsskyldigheten anges i 37 § PuL. Enligt den bestämmelsen behöver en anmälan enligt 36 § första stycket inte göras om den personuppgiftsansvarige har anmält till tillsynsmyndigheten att ett personuppgiftsombud utsetts och vem det är (jfr artikel 18.2 andra strecksatsen). Detta i praktiken betydelsefulla undantag är, till skillnad från sådana undantag som avses i 36 § tredje stycket, inte villkorat av att det ska handla om en behandlingstyp som sannolikt inte leder till otillbörligt intrång i den personliga integriteten. Systemet med personuppgiftsombud är frivilligt för myndigheter liksom för andra personuppgiftsansvariga.

Särskilt om personuppgiftsombudet

I 3 § PuL definieras personuppgiftsombud som den fysiska person som, efter förordnande av den personuppgiftsansvarige, självständigt ska se till att personuppgifter behandlas på ett korrekt och lagligt sätt. Med självständighetsrekvisitet avses detsamma som anges i direktivet om att ombudet ”på ett oberoende sätt” ska kunna säkra

den interna tillämpningen. Är ombudet anställd hos den personuppgiftsansvarige, får han eller hon inte ha en alltför underordnad ställning (prop. 1997/98:44 s. 140). Den personuppgiftsansvarige kan också anlita någon utanför den egna organisationen att vara personuppgiftsombud. Denne anses då inte vara tredje man i personuppgiftslagens mening (3 § PuL). Det finns inget som hindrar att den personuppgiftsansvarige utser flera personuppgiftsombud eller att flera personuppgiftsansvariga utser en och samma person till personuppgiftsombud (a. prop. s. 139). Datainspektionen framhåller i sin informationsbroschyr om personuppgiftsombud att det, för det fall det finns flera ombud, är bra om man beskriver ombudens inbördes arbetsfördelning och roller. Om den personuppgiftsansvarige utser ett ombud utanför sin egen organisation är det vidare lämpligt att ett avtal upprättas mellan den personuppgiftsansvarige och ombudet. Av avtalet bör framgå vilket uppdrag ombudet har och vilka arbetsuppgifter denne ska utföra.

Personuppgiftsombudets uppgifter anges i 38–40 §§ PuL. Enligt 38 § första stycket ska personuppgiftsombudet självständigt se till att den personuppgiftsansvarige behandlar personuppgifter på ett lagligt och korrekt sätt och i enlighet med god sed. Personuppgiftsombudet ska också påpeka eventuella brister för den personuppgiftsansvarige.

Har personuppgiftsombudet anledning att misstänka att den personuppgiftsansvarige bryter mot de bestämmelser som gäller för behandlingen av personuppgifter och vidtas inte rättelse så snart det kan ske efter påpekande, ska personuppgiftsombudet anmäla förhållandet till tillsynsmyndigheten (38 § andra stycket). Personuppgiftsombudet ska även i övrigt samråda med tillsynsmyndigheten vid tveksamhet om hur de bestämmelser som gäller för behandlingen av personuppgifter ska tillämpas (tredje stycket).

I 39 § PuL föreskrivs att personuppgiftsombudet ska föra en förteckning över de behandlingar som den personuppgiftsansvarige genomför och som skulle ha omfattats av anmälningsskyldighet om ombudet inte hade funnits. Förteckningen ska omfatta åtminstone de uppgifter som en anmälan enligt 36 § skulle ha innehållit (se 6 § DIFS 2013:1).

Enligt 40 § PuL ska personuppgiftsombudet hjälpa registrerade att få rättelse när det finns anledning att misstänka att behandlade personuppgifter är felaktiga eller ofullständiga. Denna bestämmelse

har ingen motsvarighet i direktivet utan är en inhemsk reglering med rötter i 1973 års datalag. Enligt 8 § fjärde stycket datalagen (1973:289) skulle en registeransvarig utse en eller flera personer som skulle bistå de registrerade vid misstanke om oriktig eller missvisande personuppgift. Sådana uppgifter skulle, enligt första stycket samma paragraf, under vissa förutsättningar rättas, ändras eller uteslutas. Enligt bestämmelsen i datalagen var det också denne person som skulle lämna underrättelse om vidtagen rättelse m.m. till en tidigare mottagare av personuppgiften i fråga, om den registrerade begärde det eller om det förelåg risk för otillbörligt intrång i personlig integritet.

Förhandskontroll

I 41 § PuL bemyndigas regeringen att meddela föreskrifter om att sådana behandlingar av personuppgifter som innebär särskilda risker för otillbörligt intrång i den personliga integriteten ska för förhandskontroll anmälas till tillsynsmyndigheten enligt 36 § tre veckor i förväg. Om regeringen har meddelat sådana föreskrifter, gäller inte undantaget från anmälningsskyldigheten enligt 37 §. Det innebär att anmälan för förhandskontroll måste göras även om den personuppgiftsansvarige har ett personuppgiftsombud. Paragrafen har införts mot bakgrund av artikel 20.1 i direktivet (prop. 1997/98:44 s. 141). Det finns numera inga gällande allmänna bestämmelser som föreskriver en sådan förhandskontroll som avses i 41 § PuL. Den 1 mars 2013 upphävdes dåvarande 10 § PuF som föreskrev anmälningsplikt och förhandskontroll för personuppgifter om genetiska anlag som framkommit efter genetisk undersökning. Sådan personuppgiftsbehandling förekommer hos myndigheter som bedriver hälso- och sjukvård eller medicinsk forskning. Däremot finns en särbestämmelse om att behandling hos Skatteverket rörande personuppgifter om brottsmisstankar ska anmälas för förhandskontroll (2 § förordningen [1999:105] om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar).

Enligt Datalagskommittén kan sådan förhandskontroll som avses i artikel 20 i direktivet av särskilt känsliga personuppgiftsbehandlingar sägas ske i samband med att registerförfattningar tas fram och beslutas av riksdag eller regering (SOU 1997:37 s. 427).

Upplysningar till allmänheten om behandlingar som inte anmälts

I 42 § PuL finns bestämmelser om upplysningar till allmänheten om behandlingar som inte anmälts till tillsynsmyndigheten. Den personuppgiftsansvarige ska till var och en som begär det skyndsamt och på lämpligt sätt lämna upplysningar om sådana automatiserade eller andra behandlingar av personuppgifter som inte har anmälts till tillsynsmyndigheten. Upplysningarna ska omfatta det som en anmälan enligt 36 § första stycket skulle ha omfattat. Den personuppgiftsansvarige är dock inte skyldig att lämna ut sekretessbelagda uppgifter eller uppgifter om vilka säkerhetsåtgärder som har vidtagits. Paragrafen är avsedd att ha samma innebörd som artikel 21.3 första stycket i direktivet (prop. 1997/98:44 s. 142). På samma sätt som enligt direktivet omfattar bestämmelsen inte bara helt eller delvis automatiserad behandling utan även behandling i manuella register. Det finns inget krav på att upplysningar ska lämnas skriftligen. I förarbetena angavs att bestämmelserna i 42 § PuL förmodligen skulle leda till att de personuppgiftsansvariga upprättar och håller aktuell någon form av förteckning över aktuella behandlingar (a. prop. s. 100). Som framgått ovan har vidare ett av undantagen från anmälningsskyldigheten enligt 36 § första stycket för viss behandling gjorts beroende av att den personuppgiftsansvarige själv för en förteckning med de uppgifter som annars skulle ha anmälts (5 § d DIFS 2013:1).

En myndighets beslut om upplysningar enligt 42 § PuL är överklagbart enligt 52 § PuL då ett sådant beslut ansetts direkt beröra den enskilde (prop. 2005/06:173 s. 51 f.). Se vidare angående frågor om överklagande avsnitt 18.3.

Bestämmelserna i 42 § PuL om upplysningar till allmänheten på begäran från en enskild behöver inte tillämpas i fråga om behandling av personuppgifter som inte ingår i eller är avsedda att ingå i en samling av personuppgifter som har strukturerats för att påtagligt underlätta sökning efter eller sammanställning av personuppgifter. Detta följer av den s.k. missbruksregeln i 5 a § PUL. Enligt förarbetena till missbruksregeln kan skyldigheten att på begäran lämna upplysningar till allmänheten om behandlingar inte anses bidra till integritetsskyddet i någon nämnvärd omfattning eller ha en sådan praktisk betydelse för de registrerade att det uppväger besväret för den personuppgiftsansvarige att lämna upplysningarna. Ett undantag

beträffande 42 § PUL för personuppgifter i ostrukturerat material ansågs därför vara motiverat (prop. 2005/06:173 s. 40).

Förslaget till uppgiftsskyddsförordning

I förslaget till uppgiftsskyddsförordning finns en hel del nyheter och förändringar i förhållande till dataskyddsdirektivet såvitt avser anmälningsskyldighet m.m. Bland annat slopas huvudregeln om anmälningsskyldighet till tillsynsmyndigheten. I stället ska personuppgiftsansvariga bevara dokumentation om behandlingar samt göra konsekvensbedömningar av planerade behandlingar som medför särskilda risker. I vissa fall krävs dock förhandstillstånd från eller samråd med tillsynsmyndigheten. Vidare införs krav på att ett uppgiftsskyddsombud utses i vissa fall samt en tydligare reglering av dennes uppgifter och ställning. Det ska observeras att den föreslagna regleringen delvis är tämligen omfattande och redogörelsen nedan är inte heltäckande. Det ska också observeras att Europaparlamentets ändringsförslag i lagstiftningsresolutionen av den 12 mars 2014 behandlas i anslutning till redogörelsen under respektive underrubrik.

Dokumentation

Enligt artikel 28 ska registeransvariga och registerförare bevara dokumentation om all behandling som de ansvarar för. Dokumentationen ska innehålla i princip motsvarande uppgifter som en anmälan till tillsynsmyndigheten enligt direktivet ska innehålla (artikel 19.1 i direktivet). Dessutom ska dokumentationen innehålla bl.a. kontaktuppgifter till eventuella registerförare, gemensamma registeransvariga eller uppgiftsskyddsombudet. En allmän anvisning om tidsfristerna för radering av de olika kategorierna av uppgifter ska också finnas liksom en beskrivning av de rutiner som avses i artikel 22.3, dvs. rutiner som införts för kontrollen av om antagna policyer och åtgärder för säkerställandet m.m. av att personuppgiftsbehandlingen utförs i enlighet med förordningen är verkningsfulla.

Den registeransvarige (och registerföraren) är skyldig att på tillsynsmyndighetens begäran göra dokumentationen tillgänglig så

att den kan tjäna som grund för övervakningen av behandlingen (artikel 28.2).

Kommissionen föreslås få befogenheter att anta delegerade akter som preciserar kriterierna och kraven för dokumentationen och att fastställa standardformulär för densamma (artikel 28.5 och 6).

Europaparlamentet har föreslagit flera strykningar avseende vilka uppgifter dokumentationen enligt artikel 28 ska innehålla. Bara kontaktuppgifter till registeransvarig och uppgiftsskyddsombudet m.m. behålls. I övrigt anges att den dokumentation som krävs för att uppfylla de krav som fastställs i förordningen ska bevaras. Här, liksom beträffande många övriga förslag i förordningen, har parlamentet strukit möjligheten för kommissionen att anta delegerade akter. Detta gäller även de övriga artiklar som berörs nedan.

Konsekvensbedömning avseende uppgiftsskydd och förhandstillstånd eller förhandssamråd

Genom artikel 33 föreslås en skyldighet för registeransvariga och registerförare att i förväg göra en konsekvensbedömning avseende uppgiftsskydd för en planerad behandling som medför särskilda integritetsrisker för de registrerade. Vidare specificeras vissa typfall som innebär särskilda integritetsrisker, exempelvis systematisk och omfattande bedömning av en fysisk person för olika syften, vissa behandlingar av känsliga personuppgifter, information från kameraövervakning från allmän plats i stor skala eller storskaliga register med uppgifter om barn, genetisk information eller biometriska data. Konsekvensbedömningen ska innehålla åtminstone en allmän beskrivning av den planerade behandlingen, en bedömning av riskerna för de registrerades fri- och rättigheter, de åtgärder som planeras för att hantera risker, skyddsåtgärder, säkerhetsåtgärder och rutiner för att garantera skyddet av personuppgifterna och för att visa att förordningen efterlevs. Den registeransvarige ska inhämta synpunkter från de registrerade och deras företrädare om den avsedda behandlingen, utan att det påverkar skyddet av kommersiella eller allmänna intressen eller behandlingens säkerhet.

Om den registeransvarige är en offentlig myndighet eller ett offentligt organ och om behandlingen följer av en rättslig skyldighet enligt artikel 6.1 c som föreskriver regler och förfaranden som rör behandlingen och regleras av unionslagstiftningen, ska kravet på

konsekvensbedömningar inte gälla, om inte medlemsstaterna anser det nödvändigt att utföra en sådan bedömning före behandlingen (artikel 33.5). Undantaget från det ovillkorliga kravet på konsekvensbedömningar omfattar således inte behandlingar som följer av rättsliga skyldigheter enligt en medlemsstats nationella lagstiftning.

Enligt punkten 72 i ingressen till förordningen kan konsekvensbedömningar avse bredare områden än ett enda projekt, exempelvis när myndigheter eller organ avser att skapa en gemensam tillämpnings- eller behandlingsplattform.

I artikel 34 – förhandstillstånd och förhandssamråd – anges de fall där tillstånd av eller samråd med tillsynsmyndigheten är obligatoriskt inför planerade behandlingar. Bestämmelserna bygger på begreppet "förhandskontroll" i artikel 20 i dataskyddsdirektivet. Förhandstillstånd av tillsynsmyndigheten krävs i vissa fall i samband med planerad överföring av personuppgifter till tredjeland eller internationell organisation (artikel 34.1). Vidare ska förhandssamråd ske med tillsynsmyndigheten om en konsekvensanalys enligt artikel 33 visat att behandlingen sannolikt medför höggradiga särskilda risker eller om behandlingen hör till en behandlingstyp för vilken tillsynsmyndigheten uppställt generella krav på förhandssamråd (artikel 34.2). Kommissionen ska få anta delegerade akter som preciserar bl.a. kriterierna för fastställandet av höggradiga särskilda risker.

Europaparlamentet har föreslagit relativt omfattande förändringar i förslaget när det gäller konsekvensbedömningar m.m. Bland annat föreslås en ny artikel 32a enligt vilken registeransvariga ska göra en riskanalys av planerade behandlingars konsekvenser för de registrerades rättigheter och friheter med en bedömning av frågan om behandlingen medför särskilda risker. Vidare preciseras vissa behandlingsformer som sannolikt medför särskilda risker. Först om en riskanalys visar att vissa av dessa slags behandlingsformer ska utföras, måste en konsekvensbedömning enligt artikel 33 göras. Den ska, till skillnad från i kommissionens förslag, uttryckligen ta hänsyn till hela ”livscykeln” avseende behandlingen av personuppgifterna, från insamling till radering. Konsekvensbedömningen ska vidare dokumenteras i enlighet med närmare och uttryckliga krav på innehållet. Enligt en ny artikel 33a ska vidare regelbunden uppföljning ske. Därutöver föreslår Europaparlamentet att kravet på förhandstillstånd i vissa fall slopas.

Uppgiftsskyddsombud

Enligt artikel 35 blir det obligatoriskt för myndigheter och vissa andra registeransvariga att utse uppgiftsskyddsombud. En offentlig myndighet får utnämna ett gemensamt ombud för flera av dess enheter. Motsatsvis följer således att en myndighet kan utse flera ombud. Ett ombud ska utnämnas för en period på minst två år. Ett uppgiftskyddsombud kan vara en extern och oberoende uppdragstagare men ombudet kan också utses bland den personuppgiftsansvariges anställda. Den registrerade ska ha rätt att kontakta uppgiftsskyddsombudet om alla frågor som rör behandlingen av den registrerades uppgifter och för att begära att få utöva sina rättigheter enligt förordningen.

Genom artikel 36 redogörs för uppgiftsskyddsombudets ställning. Det åligger den registeransvarige (eller registerföraren) att se till att ombudet deltar i alla frågor som rör skyddet av personuppgifter, att ombudet kan utföra sitt uppdrag på ett oberoende sätt och ges stöd i form av personal och utrustning m.m. som krävs för uppdraget.

Genom artikel 37 preciseras och utvidgas ombudets uppgifter i förhållande till direktivet. En av flera uppgifter för ombudet är att övervaka genomförandet och tillämpningen när det gäller de krav som avser inbyggt uppgiftsskydd, uppgiftsskydd som standard och datasäkerhet samt konsekvensbedömningar. Ombudet ska vidare fungera som kontaktpunkt i förhållande till tillsynsmyndigheten.

Europaparlamentet har endast föreslagit smärre tillägg eller förändringar i kommissionens förslag när det gäller frågor om uppgiftsskyddsombud. Av intresse här är närmast förslaget till tillägg i artikel 36 om att uppgiftsskyddsombudet ska omfattas av tystnadsplikt rörande de registrerades identitet och sådana omständigheter som gör det möjligt att identifiera dem, om de inte befrias från denna skyldighet av de registrerade.

Några kommentarer

Det kan konstateras att den föreslagna uppgiftsskyddsförordningen innehåller ett flertal krav som innebär nyheter eller förtydliganden i förhållande till vad som för närvarande gäller enligt dataskyddsdirektivet och personuppgiftslagen.

Ordningen med dokumentation i stället för anmälan till tillsynsmyndigheten innebär minskad administration framför allt för tillsynsmyndigheterna men sannolikt i viss mån även för personuppgiftsansvariga. Det är dock svårt att uppskatta vilken betydelse i praktiken förändringen skulle få för personuppgiftsbehandlande myndigheter. Några anpassningssvårigheter torde dock inte uppstå. Visserligen riktas det föreslagna kravet om att bevara dokumentation även mot myndigheter som är personuppgiftsbiträden. Det torde dock vara den personuppgiftsansvariga myndigheten som har att upprätta den dokumentation som personuppgiftsbiträdet måste bevara.

De uttryckliga kraven på konsekvensbedömningar avseende uppgiftsskydd inför planerade behandlingar som medför särskilda risker för den registrerades fri- och rättigheter är visserligen ett nytt krav jämfört med direktivet. Med tanke på vad för slags behandlingstyper som enligt uppgiftsskyddsförordningen kräver konsekvensbedömningar är det emellertid vår preliminära bedömning att regelverket redan i dagsläget implicit kräver den sortens bedömningar när en myndighet initierar en behandling av det slaget i den mån myndigheten alls kan hämta rättsligt stöd för att utföra sådan behandling i regleringen av myndighetens uppgifter och verksamhet. Det är alltså vår bedömning att myndigheter inte heller enligt gällande rätt kan påbörja särskilt integritetskänsliga personuppgiftsbehandlingar utan att först ha gjort en riskbedömning och en bedömning av vilka säkerhetsåtgärder som krävs. Vad som förefaller i viss mån problematiskt är emellertid att konsekvensbedömningar ska göras även när myndighetens behandling följer av en rättslig skyldighet i lag eller förordning, t.ex. på grund av att riksdagen har beslutat genom lag att ett visst register med visst innehåll ska föras. Som framgått ovan är det bara när den rättsliga skyldigheten för den registeransvariga myndigheten följer av unionslagstiftningen som myndigheten inte behöver göra någon konsekvensbedömning (artikel 33.5) Det ter sig emellertid något udda för svenska förhållanden att en myndighet skulle behöva göra en egen konsekvensbedömning av bl.a. riskerna för de registrerades fri- och rättigheter trots att det i det bakomliggande lagstiftningsärendet redan gjorts en avvägning mellan intresset av registerföringen och motstående risker för integritetsintrång. Ett ytterligare förhållande när det gäller förslaget om konsekvensbedömningar som det finns skäl att notera är att det ter

sig allmänt sett oklart hur myndigheter ska inhämta synpunkter från registrerade om avsedda behandlingar och vilka administrationskostnader m.m. som det förslaget kan medföra (artikel 33.4).

Förslaget om att det ska bli obligatoriskt för myndigheter att utse ett uppgiftsskyddsombud kommer att innebära förändringar i vart fall för sådana myndigheter som inte redan har personuppgiftsombud. Det finns t.ex. många myndigheter som inte sysslar med integritetskänslig eller omfattande personuppgiftsbehandling och som i dag saknar sådant ombud.

Det kan vidare nämnas att Europaparlamentets förslag om tystnadsplikt för personuppgiftsombud generellt sett inte skulle överensstämma med vad som följer av sekretessregleringen i offentlighets- och sekretesslagen. För det fall det handlar om personuppgifter som är offentliga hos myndigheten kan det konstateras att det i dag inte finns någon bestämmelse om att myndighetens personuppgiftsombud skulle ha tystnadsplikt eller att personuppgifter skulle omfattas av sekretess vid ombudets hantering av dem. En anpassning i offentlighets- och sekretesslagen torde därför behöva övervägas om den föreslagna tystnadsplikten genomförs i en kommande förordning. Om och i så fall hur en sådan anpassning bör ske torde vara en inte helt okomplicerad fråga.

Slutligen kan konstateras att uppgiftsskyddsförordningen inte innehåller någon motsvarighet till artikel 21 i dataskyddsdirektivet om behandlingars offentlighet. Enligt förordningen finns alltså ingen skyldighet för registeransvariga att lämna information om behandlingar till var och en som begär det.

16.2 Reglering i registerförfattningar

Registerförfattningar innehåller normalt inga bestämmelser om anmälningsskyldighet till tillsynsmyndigheten. I den mån frågan över huvud taget kommenteras hänvisas i allmänhet till att bestämmelsen i 3 § 3 PuF – där det föreskrivs att behandling av personuppgifter som regleras genom särskilda föreskrifter i lag eller förordning inte omfattas av anmälningsskyldighet – innebär att någon anmälan inte behöver göras (se t.ex. prop. 2000/01:33 s. 95 och prop. 2009/10:85 s. 88). Inte i någon av de informationshanteringsförfattningar som är konstruerade på det sättet att de uttryckligen hänvisar till olika

bestämmelser i personuppgiftslagen som ska vara tillämpliga vid personuppgiftsbehandling enligt registerförfattningen i fråga hänvisas till personuppgiftslagens huvudregel om anmälningsskyldighet (36 § PuL) eller de olika undantagen från anmälningsskyldigheten (se t.ex. 2 kap. 2 § polisdatalagen [2010:361]). Resonemangen bakom dessa konstruktioner ter sig dock inte helt konsekventa. Å ena sidan ska bestämmelserna i 36 § om anmälningsskyldighet och bemyndigande för regeringen att meddela undantag inte vara tillämpliga. Å andra sidan motiveras bedömningarna om att anmälan inte behöver göras vid behandling enligt lagen i fråga med en undantagsbestämmelse i personuppgiftsförordningen som regeringen meddelat med stöd just av bemyndigandet i 36 § PuL.

Som huvudregel gäller enligt registerförfattningarna personuppgiftslagens bestämmelser om möjligheten att utse ett personuppgiftsombud. Endast i några författningar – lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst, lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet samt polisdatalagen och kustbevakningsdatalagen – har det gjorts obligatoriskt för den personuppgiftsansvarige att utse ett eller flera ombud. I förarbetena till polisdatalagen anförde regeringen att integritetskänsligheten i behandlade uppgifter gör det särskilt angeläget med den kontroll som kan utövas av ett personuppgiftsombud. Vidare framhölls vikten av att enskilda registrerade enkelt kan vända sig till rätt person hos myndigheten i bl.a. frågor om information om behandlingen och om rättelse av felaktiga uppgifter (prop. 2009/10:85 s. 93). Även förslaget till domstolsdatalag innehåller ett krav på att det ska bli obligatoriskt för domstolarna att utse personuppgiftsombud (Ds 2013:10).

Det förefaller inte finnas några gällande registerförfattningar vars bestämmelser i sak avviker från vad personuppgiftslagen anger om ombudets uppgifter i 38–40 §§ PuL. Dessa gäller således även på registerförfattningsreglerade områden. Förslaget till domstolsdatalag avviker dock i det avseendet att personuppgiftsombudet inte ska ha i uppgift att föra en förteckning över behandlingar som skulle ha omfattats av anmälningsskyldighet enligt 36 § första stycket PuL om ombudet inte hade funnits. I förslaget har det därför inte gjorts någon hänvisning till 39 § PuL. Det sammanhänger med att det i

stället föreslås att den personuppgiftsansvariga domstolen ska föra en motsvarande förteckning.

För flertalet registerförfattningsreglerade myndigheter torde det inte bli aktuellt med sådan behandling av särskilt integritetskänsliga behandlingar som avses i 41 § PuL och beträffande vilka regeringen kan föreskriva om anmälningsplikt för förhandskontroll. Icke desto mindre brukar det hänvisas till att 41 § PuL ska vara tillämplig i sådana registerförfattningar som konstruerats på det sättet att hänvisning sker till de bestämmelser i personuppgiftslagen som ska vara tillämpliga då personuppgifter behandlas enligt registerlagen i fråga. Det har således bedömts att regeringen bör ha den möjligheten (se t.ex. prop. 2000/01:33 s. 96). Lagarna om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst respektive Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet är de enda författningar som helt saknar bestämmelser rörande förhandskontroll. Dessa författningar avser dock verksamhetsområden som faller utanför unionsrättens tillämpningsområde. Det torde vidare kunna hävdas att verksamheterna är tillräckligt reglerade som de är då de per definition avser känsliga behandlingar.

Vad slutligen gäller upplysningar till allmänheten är bestämmelserna i 42 § PuL normalt tillämpliga även vid behandling av personuppgifter enligt olika registerförfattningar. I förarbeten har ofta endast anförts att det är väsentligt att den enskilde på ett enkelt sätt kan få besked om vilka behandlingar som utförs av myndigheterna även om de inte omfattas av någon anmälningsskyldighet till tillsynsmyndigheten (se t.ex. prop. 2009/10:85 s. 89).

16.3 Andra bestämmelser om information till allmänheten m.m.

I avsnitt 13.3 har vi berört handlingsoffentlighetens betydelse för den registrerades möjligheter att få närmare insyn i myndigheters behandling av personuppgifter om honom eller henne. Rätten att ta del av allmänna handlingar har givetvis en vidare betydelse än så och innebär en princip om offentlighet i myndigheternas informationshantering som sedan länge gällt i Sverige. Här kan också påminnas om myndigheternas serviceskyldighet och grundläggande skyldighet

att på begäran lämna uppgifter ur allmänna handlingar (4 § FL samt 6 kap. 4 och 6 § OSL).

På myndighetsområdet finns alltså bestämmelser i grundlag som innebär en möjlighet att följa och kontrollera myndigheternas informationshantering genom att ta del av allmänna handlingar. Det finns också bestämmelser i vanlig lag som ställer krav på att myndigheter ska kunna tillhandahålla allmänheten och övriga intressenter övergripande redovisning av vilken informationshantering som myndigheterna ägnar sig åt. Denna reglering gäller parallellt med personuppgiftslagens reglering av vilken information om behandlingar som ska anmälas till tillsynsmyndigheten eller förtecknas och kunna lämnas till var och en som begär det.

En central bestämmelse i detta sammanhang är 4 kap. 2 § OSL. Av den paragrafen följer att varje myndighet ska upprätta en beskrivning av myndighetens allmänna handlingar som ska vara tillgänglig för allmänheten och som ger information om

1. myndighetens organisation och verksamhet i syfte att underlätta sökande efter allmänna handlingar,
2. register, förteckningar eller andra sökmedel till myndighetens allmänna handlingar,
3. tekniska hjälpmedel som enskilda själva kan få använda hos myndigheten för att ta del av allmänna handlingar,
4. vem hos myndigheten som kan lämna närmare upplysningar om myndighetens allmänna handlingar, deras användning och sökmöjligheter,
5. vilka bestämmelser om sekretess som myndigheten vanligen tillämpar på uppgifter i sina handlingar,
6. uppgifter som myndigheten regelbundet hämtar från eller lämnar till andra samt hur och när detta sker, och
7. myndighetens rätt till försäljning av personuppgifter.

Syftet med beskrivningarna är framför allt att underlätta för enskilda som vill utnyttja sin grundlagsstadgade rätt att få ta del av myndigheternas allmänna handlingar. Kravlistan tillmötesgår vidare i praktiken flera av de krav på vad en anmälan enligt 36 § PuL till

tillsynsmyndigheten ska innehålla och därmed hur och om vad allmänheten ska kunna få upplysningar enligt 42 § PuL.

Bestämmelserna i 4 kap. 2 § OSL är sedan offentlighets- och sekretesslagens införande år 2009 teknikneutrala men omfattade i 1980 års sekretesslag enbart myndigheters ADB-register (15 kap. 9 och 11 §§ SekrL). En annan skillnad är att beskrivningen inte längre behöver omfatta uppgifter om ett ADB-registers benämning eller om dess ändamål. På så vis har överlappningen minskat mellan sekretesslagstiftningens beskrivning av myndighetens allmänna handlingar och personuppgiftslagens krav på information till allmänheten. Det är numera bara 42 § PuL som uttryckligen föreskriver att information om ändamålen för behandlingar i personregister m.m. måste ges.

Inte heller finns det längre något uttryckligt krav på beskrivning av vilka typer av uppgifter i ADB-register som myndigheten har tillgång till. Däremot gäller fortfarande ett krav på att myndigheten bl.a. redovisar vilken direktåtkomst myndigheten har till andra aktörers informationssamlingar och myndighetens eget utlämnande av uppgifter genom direktåtkomst. Det framgår av 4 kap. 2 § första stycket 6 OSL. Bestämmelsen omfattar dock inte bara krav på redovisning av vilken direktåtkomst som förekommer. Även annat regelmässigt informationsutbyte ska redovisas. Enligt motiven är det särskilt viktigt att upplysningar ges om information lämnas till eller hämtas från andra utan den registrerades medverkan (prop. 1990/91:60 s. 77). Här finns en tydlig överlappning såvitt avser bestämmelserna i 42 § PuL och de närmare föreskrifter som finns om vad informationen enligt den bestämmelsen ska innehålla.

Punkten 7 i 4 kap. 2 § första stycket OSL syftar till att ge registrerade möjligheter att få reda på om uppgifter om dem säljs av myndigheterna (a. prop. s. 56). Genom placeringen i offentlighets- och sekretesslagen är redovisningsskyldigheten i detta avseende inte begränsad till elektronisk informationshantering eller behandling i manuella register (jfr 5 § PuL). Frågan är dock vilken betydelse skillnaden i regleringarnas tillämpningsområde har i praktiken. Av allt att döma torde det numera enbart förekomma försäljning av sammanställda personuppgifter som behandlas helt eller delvis automatiserat. Man kan därför tycka att, med det syfte punkten 7 har, bestämmelsen rent systematiskt skulle passa bättre i en reglering av myndigheters behandling av personuppgifter.

Av vikt för allmänhetens insyn i myndigheters personuppgiftsbehandlingar är vidare bestämmelserna om att allmänna handlingar som regel ska registreras (5 kap. 1 och 2 §§ OSL), att de ska hållas ordnade och, vad gäller elektronisk information, att därvid ska beaktas det intresse som enskilda kan ha av att själva utnyttja tekniska hjälpmedel hos myndigheter för att ta del av allmänna handlingar (4 kap. 1 § OSL).

Slutligen kan nämnas bestämmelsen i 6 § arkivlagen (1990:782) enligt vilken det ingår i arkivvården att en myndighet ska organisera arkivet på ett sådant sätt att rätten att ta del av allmänna handlingar underlättas (punkt 1). Dessutom ska myndigheten upprätta dels en arkivbeskrivning som ger information om vilka slag av handlingar som kan finnas i myndighetens arkiv och hur arkivet är organiserat, dels en systematisk arkivförteckning (punkt 2). För statliga myndigheter gäller dessutom särskilda krav på hur en myndighet ska dokumentera sina elektroniska handlingar (5 kap. RA-FS 2009:1).

Sammanfattningsvis kan konstateras att de bestämmelser som finns i offentlighets- och sekretesslagen samt arkivlagen, direkt eller indirekt, sammantaget får anses uppfylla väsentliga delar av de krav på information som följer av bestämmelserna i dataskyddsdirektivet om att behandlingarna ska göras offentliga (artikel 21) och som i huvudsak genomförts i Sverige genom 42 § PuL. Det mervärde som den bestämmelsen ger är att informationen koncentreras till just personuppgifter och, inte minst, att myndigheterna måste tydliggöra för vilka ändamål man samlar in och sedan behandlar personuppgifter i sin verksamhet.

16.4 Våra överväganden och förslag

16.4.1 Anmälningsskyldighet m.m.

Förslag: Myndigheters behandling av personuppgifter enligt den nya lagen ska inte omfattas av anmälningsskyldighet till tillsynsmyndigheten. Myndigheterna ska i stället föra förteckningar över de behandlingar som utförs med stöd av lagen. Förteckningarna avses innehålla motsvarande uppgifter som en anmälan till tillsynsmyndigheten enligt 36 § PuL skulle ha innehållit. Närmare

föreskrifter om förteckningarnas innehåll bör meddelas av regeringen eller myndighet som regeringen bestämmer.

Formellt omfattas alltså även den offentliga sektorns personuppgiftsbehandling av personuppgiftslagens huvudregel om att behandlingar ska anmälas till tillsynsmyndigheten. Olika undantagsbestämmelser medför emellertid sammantaget att stora delar av myndigheternas personuppgiftsbehandling inte behöver anmälas. Detta gäller inte bara registerförfattningsreglerade verksamheter. Flertalet undantagsbestämmelser, se ovan i avsnitt 16.1, omfattar alla myndigheter oavsett om deras personuppgiftsbehandling omfattas av registerförfattningar eller inte. Frånsett undantaget i 37 § PuL om att utseendet av ett personuppgiftsombud medför att anmälan enligt 36 § inte behöver göras, bygger bestämmelserna på bedömningen att undantagen avser sådana typer av behandlingar som sannolikt inte kommer att leda till otillbörliga intrång i den personliga integriteten eller att de registrerades fri och rättigheter kränks (jfr 36 § tredje stycket PuL och artikel 18.2 första strecksatsen i direktivet).

Personuppgiftsbehandling är en integrerad del i myndigheternas utförande av sina författningsreglerade uppgifter och befogenheter. Rent generellt anser vi att det måste vara en utgångspunkt att myndigheters behandling av personuppgifter normalt sett inte innebär kränkning av de registrerades fri- och rättigheter. Det är vidare vår bedömning att anmälningsskyldigheten i sig inte bidrar till ett förbättrat integritetsskydd, i vart fall inte på myndigheternas område, utan snarare framstår som en tämligen udda företeelse i det sammanhanget. Stora delar av personuppgiftsbehandlingen är särskilt reglerad genom uttryckliga bestämmelser om registrering, informationsutbyte m.m. Detta gäller regelmässigt beträffande sådan behandling som är särskilt känslig från integritetssynpunkt. Även i anslutning till den nya lagen kommer det att finnas särbestämmelser som klargör vad som gäller på vissa specifika områden. Mot den bakgrunden anser vi att det är motiverat att generellt undanta all personuppgiftsbehandling hos myndigheter från anmälningsskyldighet.

Dataskyddsdirektivet kan emellertid förefalla kräva, för att undantag från anmälningsskyldighet ska kunna föreskrivas, att medlemsstaterna i sin nationella lagstiftning också slår fast behandlingstypens ändamål, vilka uppgiftskategorier som behandlas och vilka kategorier registrerade som avses m.m. (artikel 18.2 första streck-

satsen). Sådana preciserade bestämmelser kommer den nya lagen inte att innehålla. Vi menar dock att bestämmelsen i direktivet måste läsas i ljuset av det bakomliggande syftet med anmälningsförfarandet. Av punkt 48 i ingressen framgår att meningen är att göra behandlingens syfte och viktigaste egenskaper allmänt kända, vilket i sin tur ska säkerställa att behandlingen sker i enlighet med personuppgiftsskyddsregleringen. Det huvudsakliga syftet kan alltså antas vara att skapa offentlighet åt anmälda behandlingar. Det är t.ex. därför tillsynsmyndigheter ska föra ett allmänt tillgängligt register över anmälda behandlingar (artikel 21.2 och 7 § PuF). Någon kontroll eller prövning av anmälda behandlingars laglighet eller liknande ska däremot inte göras.

Förutsatt att det i den nationella rätten finns garantier för att behandlingens syfte och viktigare egenskaper blir allmänt kända, är det alltså vår uppfattning att det inte strider mot direktivet att generellt undanta myndigheters behandling av personuppgifter från kravet på anmälningsskyldighet då utgångspunkten får anses vara att dessa behandlingar, normalt sett, inte medför kränkningar av de registrerades fri- och rättigheter.

För att uppnå samma syfte som med anmälningsförfarandet, dvs. att göra information om behandlingarna offentligt tillgänglig, bör varje myndighet i stället åläggas att sammanställa information om sina personuppgiftsbehandlingar i en förteckning som regelbundet uppdateras. Utgångspunkten bör därmed vara att förteckningen ska innehålla i vart fall samma information som en anmälan till tillsynsmyndigheten skulle ha innehållit enligt artikel 19 i direktivet. Vidare bör information kunna lämnas om t.ex. personuppgiftsombudets kontaktuppgifter och myndigheters rätt att sälja personuppgifter. Vad gäller det sistnämnda har vi tidigare anfört att bestämmelsen i 4 kap. 2 § 7 OSL om att myndigheters information om allmänna handlingar ska innehålla uppgift om myndighetens rätt att försälja personuppgifter systematiskt sett skulle passa bättre i en reglering av myndigheters behandling av personuppgifter. Den nya lag vi föreslår omfattar emellertid inte samtliga statliga och kommunala myndigheter. Redan av det skälet ser vi ingen anledning att föreslå en flytt av bestämmelsen från offentlighets- och sekretesslagen till den nya lagen. Det utesluter givetvis inte att en sådan förteckning som vi föreslår ändå innehåller motsvarande information.

Närmare föreskrifter om förteckningens innehåll bör inte ges i lag utan i förordning eller genom myndighetsföreskrifter. Det är dock väsentligt att framhålla att skyldigheten att föra en förteckning inte är avsedd att medföra någon egentlig meradministration för myndigheterna, vilket får beaktas i utformningen av föreskrifterna om vad förteckningarna ska innehålla. I det sammanhanget kan vidare konstateras att det i praktiken redan torde gälla att myndigheter måste ha något slags förteckning av de avsedda uppgifterna med tanke på vad som föreskrivs i 42 § PuL om upplysningar till allmänheten om behandlingar som inte anmälts.

Ansvaret för att det förs en korrekt förteckning över myndighetens personuppgiftsbehandlingar bör ligga hos myndigheten. Eftersom det enligt personuppgiftslagen är personuppgiftsombudet, inte den personuppgiftsansvariga myndigheten, som ska föra motsvarande förteckning kan, i vart fall hypotetiskt, annars den situationen tänkas uppstå att, om en myndighet har anlitat en extern uppdragstagare att vara personuppgiftsombud, förteckningen inte blir allmän handling hos myndigheten. Att myndigheten själv ansvarar för förteckningen har vidare den fördelen att förteckningen, och arbetet med den, kan samordnas med de beskrivningar av myndighetens allmänna handlingar och arkiv som ändå ska finnas enligt offentlighets- och sekretesslagen respektive arkivlagen. Det torde öka informationsvärdet för enskilda och underlätta rent arbetsmässigt för myndigheterna med ett samordnat framställande av dokumenten. En förteckning som myndigheten själv för kan vidare enkelt publiceras på myndighetens webbplats.

Sammanfattningsvis anser vi alltså att myndigheters behandling av personuppgifter enligt den nya lagen inte ska omfattas av anmälningsskyldighet till tillsynsmyndigheten. Vi föreslår i stället att det införs en bestämmelse av vilken det framgår att myndigheter åläggs att föra en förteckning över de behandlingar som utförs med stöd av lagen. Förteckningen avses innehålla motsvarande uppgifter som en anmälan till tillsynsmyndigheten enligt 36 § PuL skulle ha innehållit.

Det kan emellertid för särskilda fall finnas behov av särreglering innebärande krav på förhandskontroll. Som kommer att framgå av det följande föreslår vi relativt generella bemyndiganden för regeringen – med möjlighet till vidaredelegation – att meddela föreskrifter i olika frågor, se avsnitt 18.2. Redan här kan därvid sägas att

föreskrifter om förhandskontroll av behandlingar av särskilt integritetskänsliga behandlingar ryms inom de föreslagna generella bemyndigandena. Någon hänvisning till 41 § PuL behövs därför inte.

16.4.2 Personuppgiftsombud

Förslag och bedömning: Det bör inte införas någon generell skyldighet för myndigheter att utse personuppgiftsombud. Med undantag för föreskrifterna om ett personuppgiftsombuds uppgift att föra en särskild förteckning över myndighetens behandlingar, ska personuppgiftslagens bestämmelser om personuppgiftsombudets uppgifter gälla även enligt den nya lagen. Detta bör framgå genom hänvisningar till 38 och 40 §§ PuL.

Personuppgiftsombudet fyller en viktig funktion för integritetsskyddet vid behandling av personuppgifter. Dels bidrar ombudet genom den kontroll över myndighetens behandling som denne utför enligt 38 § PuL. Dels har ombudet en viktig roll gentemot den registrerade som kan få hjälp av ombudet då det är aktuellt med rättelse, se 40 § PuL. Till detta kommer att personuppgiftsombudet har en vidare betydelse för att skapa ett allsidigt personuppgiftsskydd än vad som direkt framgår av de nämnda bestämmelserna. Ett personuppgiftsombud kan antas få särskilda kunskaper om personuppgiftsfrågor och kan därför ge god service åt enskilda som behöver hjälp för att kunna ta tillvara sina rättigheter. Personuppgiftsombudet kan också bidra till kunskapsspridning inom den egna myndigheten och vara ett stöd för andra medarbetare (se Ds 2013:10 s. 162).

Det ter sig naturligt att myndigheter som behandlar personuppgifter i en inte obetydlig omfattning bör ha ett personuppgiftsombud. När myndigheter samarbetar i informationssystem som är gemensamma för flera myndigheter eller samarbetar för att tillhandahålla enskilda sammanhållna e-tjänster, kan det vidare finnas behov av ett personuppgiftsombud som kan se till helheten och hjälpa enskilda registrerade i förhållande till samtliga inblandade myndigheter. Som vi ser det finns det inget hinder mot att myndigheter t.ex. i ett avgränsat e-förvaltningssamarbete ”delar” ett personuppgiftsombud med uppdraget koncentrerat till personuppgiftsbehandlingen rörande detta avgränsade samarbete.

Detta skulle kunna tala för att det på myndighetsområdet inte borde vara frivilligt att utse ett personuppgiftsombud utan att huvudregeln skulle vara ett krav på att så ska ske. Samtidigt finns det myndigheter vars storlek knappast motiverar ett krav av det slaget. Det finns också myndigheter som inte hanterar personuppgifter om enskilda annat än i ringa utsträckning eller där uppgifterna i vart fall inte är av integritetskänslig art. Även sådana myndigheter kommer att omfattas av den nya lagens tillämpningsområde. Det har i vårt arbete inte kommit fram några konkreta uppgifter om att den nuvarande frivilligheten i fråga om personuppgiftsombud medför negativa konsekvenser för personuppgiftsskyddet eller i något annat avseende. Vi anser mot denna bakgrund att det inte är påkallat att införa ett generellt krav på att myndigheter ska ha ett eller flera personuppgiftsombud. Det hindrar naturligtvis inte att det på särskilda områden eller inom särskilda sektorer måhända kan visa sig vara påkallat att uppställa ett sådant krav.

Enligt vår bedömning bör således den nuvarande möjligheten att utse personuppgiftsombud gälla även vid myndigheters behandling av personuppgifter enligt den nya lagen. Personuppgiftsombudets arbetsuppgifter och skyldigheter bör vara desamma som vad som gäller enligt personuppgiftslagen, dock med undantag för skyldigheten att föra en förteckning. Att ombudet själv för en förteckning kan visserligen ofta vara befogat med hänsyn till ombudets uppgifter. Vi ser dock ingen anledning att i lag slå fast en skyldighet för ett eventuellt personuppgiftsombud att föra en separat förteckning utöver den förteckning som vi ovan föreslagit att den personuppgiftsansvariga myndigheten ska ansvara för. Vad som ska gälla i här berörda avseenden bör framgå genom hänvisningar till 38 och 40 §§ PuL.

Det föreslagna generella undantaget från anmälningsskyldigheten är inte är kopplat till frågan om det finns ett personuppgiftsombud eller inte. Det är därmed inte längre givet att utseende och entledigande av personuppgiftsombud ska anmälas till tillsynsmyndigheten (jfr 36 § andra stycket PuL). Visserligen är den nuvarande ordningen med anmälan till Datainspektionen av personuppgiftsombud till stor nytta för såväl ombuden som myndigheterna eftersom det etablerar en kontakt med inspektionen som personuppgiftsombudet har behov av i sitt uppdrag, t.ex. då det blir aktuellt att samråda vid tveksamheter (38 § tredje stycket PuL). Vidare anordnar Datainspektionen

kurser och liknande för personuppgiftsombud vilka bjuds in genom riktade utskick. Även information distribueras direkt till anmälda personuppgiftsombud. Vi menar dock att detta inte motiverar att anmälningar ska vara ett lagkrav. De behov av kontakt som här nämnts torde kunna tillgodoses utan en sådan reglering.

16.4.3 Upplysningar till allmänheten

Bedömning: Det behövs inte någon särskild bestämmelse om att upplysningar om behandlingar ska ges till var och en som begär det. Rätten att med stöd av 2 kap. TF få ta del av den förteckning över personuppgiftsbehandlingar som varje personuppgiftsansvarig myndighet ska upprätta tillgodoser dataskyddsdirektivets krav i detta hänseende.

Som har framgått följer av artikel 21.3 i dataskyddsdirektivet att medlemsstaterna ska föreskriva att registeransvariga på lämpligt sätt tillhandahåller var och en som begär det information om uppgifter som undantagits från anmälningsskyldighet. Informationen ska omfatta det som en anmälan till tillsynsmyndigheten skulle ha omfattat, dock inte allmänna uppgifter om säkerhetsåtgärder.

Som vi ser det ger emellertid redan rätten att ta del av allmänna handlingar enligt 2 kap. TF i kombination med bestämmelserna om beskrivningar av allmänna handlingar i offentlighets- och sekretesslagen samt arkivlagen goda förutsättningar för insyn i myndigheternas personuppgiftsbehandlingar. Till det kommer den förteckning över personuppgiftsbehandlingar som vi föreslår att varje myndighet ska föra. Genom att den förteckningen blir allmän handling tillgodoses, menar vi, direktivets krav i detta hänseende. Vårt förslag om myndigheters skyldighet att upprätta en förteckning över sina personuppgiftsbehandlingar ska således ses som en sådan föreskrift som avses i artikel 21.3. Att själva utlämnandet till ”var och en” sker till följd av en grundlagsstadgad rättighet för enskilda kan knappast anses innebära att direktivets syfte inte uppnås. Vi föreslår därför inte någon hänvisning till 42 § PuL eller någon motsvarande bestämmelse om upplysningar till allmänheten.

17 Tillsynsmyndighetens befogenheter i förhållande till myndigheter

17.1 Allmänna dataskyddsrättsliga regler

Dataskyddsdirektivet

I artikel 28:1–7 dataskyddsdirektivet finns bestämmelser om tillsynsmyndighet som ska finnas i respektive medlemsstat. Nedan redogörs för de bestämmelser som har betydelse för tillsynen av myndigheters behandling av personuppgifter.

Enligt artikel 28.1 ska varje medlemsstat se till att det utses en eller flera myndigheter som har till uppgift att inom dess territorium övervaka tillämpningen av de bestämmelser som medlemsstaterna antar till följd av direktivet. Dessa myndigheter ska fullständigt oberoende utöva de uppgifter som åläggs dem.

I artikel 28.3 föreskrivs att varje tillsynsmyndighet ska ha undersökningsbefogenheter. Som exempel på sådan befogenhet nämns att få tillgång till uppgifter som blir föremål för behandling och befogenhet att inhämta alla uppgifter som är nödvändiga för att sköta tillsynen.

Myndigheten ska enligt samma artikel också ha effektiva befogenheter att ingripa. Exempel på sådana befogenheter är enligt direktivet att kunna avge yttranden om behandlingar som bör kräva förhandskontroll enligt artikel 20, att kunna besluta om blockering, utplåning eller förstöring av uppgifter, att kunna besluta om tillfälligt eller slutligt förbud mot behandling, att kunna ge den registeransvarige varning eller tillrättavisning eller att kunna hänvisa saken till nationella parlament eller till andra politiska institutioner.

Vidare sägs i artikel 28:3 att sådana beslut av tillsynsmyndigheten som går en part emot kan överklagas till domstol.

I artikel 28.4 finns bestämmelser om var och ens rätt att hos tillsynsmyndigheten begära dels skydd för sina personuppgifter, dels att en kontroll görs av om en behandling är tillåten. I båda fallen finns också en rätt att få besked om vilka följder en begäran har fått.

Enligt artikel 28.6 har en nationell tillsynsmyndighet, oavsett vilken nationell lagstiftning som gäller för den aktuella behandlingen, behörighet att inom sin egen medlemsstats territorium utöva de befogenheter som i enlighet med punkt 3 åligger den. Varje myndighet kan av en myndighet i en annan medlemsstat anmodas att utöva sina befogenheter.

Tillsynsmyndigheternas ledamöter och personal ska enligt artikel 28.7 ha tystnadsplikt med avseende på förtrolig information som de har tillgång till.

Personuppgiftslagen m.m.

Bestämmelserna

Bestämmelserna i artikel 28.3 har genomförts i svensk lagstiftning genom 43 § PuL enligt vilken tillsynsmyndigheten har rätt att för sin tillsyn på begäran få

a) tillgång till de personuppgifter som behandlas,

b) upplysningar om och dokumentation av behandlingen av personuppgifter och säkerheten vid denna,

c) tillträde till sådana lokaler som har anknytning till behandlingen av personuppgifter.

I 44–47 §§ PuL finns bestämmelser som syftar till att genomföra direktivets krav i artikel 28.3 på att tillsynsmyndigheten ska ha effektiva befogenheter att ingripa.

Enligt 44 § PuL får tillsynsmyndigheten vid vite förbjuda den personuppgiftsansvarige att behandla personuppgifter på något annat sätt än genom att lagra dem, om myndigheten inte efter en begäran enligt 43 § kan få tillräckligt underlag för att konstatera att behandlingen av personuppgifter är laglig.

Vidare följer av 45 § första stycket PuL att tillsynsmyndigheten genom påpekanden eller liknande förfaranden ska försöka åstadkomma rättelse, om myndigheten konstaterar att personuppgifter behandlas eller kan komma att behandlas på ett olagligt sätt. Går det inte att få rättelse på något annat sätt eller är saken brådskande får myndigheten vid vite förbjuda den personuppgiftsansvarige att fortsätta att behandla personuppgifterna på något annat sätt än genom att lagra dem. I andra stycket föreskrivs att myndigheten också har befogenhet att föreskriva vite om den personuppgiftsansvarige inte frivilligt följer ett beslut om säkerhetsåtgärder enligt 32 § som vunnit laga kraft.

I 46 § PuL föreskrivs som huvudregel att den personuppgiftsansvarige ska ha fått tillfälle att yttra sig innan tillsynsmyndigheten beslutar om vite enligt 44 och 45 §§. Om saken är brådskande, får myndigheten dock i avvaktan på yttrandet meddela ett tillfälligt beslut om vite. Det tillfälliga beslutet ska omprövas, när yttrandetiden har gått ut.

Enligt 47 § PuL får tillsynsmyndigheten hos förvaltningsrätten inom vars domkrets tillsynsmyndigheten är belägen ansöka om att sådana personuppgifter som har behandlats på ett olagligt sätt ska utplånas.

Av 51 § PuL följer att tillsynsmyndighetens beslut enligt denna lag om annat än föreskrifter får överklagas hos allmän förvaltningsdomstol. Tillsynsmyndigheten får bestämma att dess beslut ska gälla även om det överklagas.

Enligt 2 § PuF, är Datainspektionen tillsynsmyndighet enligt personuppgiftslagen.

Enligt 1 § förordningen (2007:975) med instruktion för Datainspektionen är inspektionens uppgift att verka för att människor skyddas mot att deras personliga integritet kränks genom behandling av personuppgifter och för att god sed iakttas i kreditupplysnings- och inkassoverksamhet. Myndigheten ska särskilt inrikta sin verksamhet på att informera om gällande regler samt ge råd och hjälp åt personuppgiftsombud enligt personuppgiftslagen. Vidare hänvisas i 2 § till att det i 2 § PuF finns bestämmelser om Datainspektionens uppgifter enligt personuppgiftslagen

Av 32 kap. 1 § OSL följer att sekretess gäller hos Datainspektionen i ärende om tillstånd eller tillsyn som enligt lag eller annan författning ska handläggas av inspektionen för uppgift om enskilds

personliga eller ekonomiska förhållanden, om det kan antas att den enskilde eller någon närstående till denne lider skada eller men om uppgiften röjs. Enligt 2 § gäller motsvarande sekretess hos Justitiekanslern, om den myndigheten får en uppgift som är sekretessreglerad enligt 1 §.

Närmare om Datainspektionens befogenheter

I förarbetena till bestämmelserna i personuppgiftslagen om tillsynsmyndighetens uppgifter och befogenheter anförde regeringen att föreskrifter i dessa ämnen kan i flera fall ges i förordning och att regeringen avsåg att senare meddela sådana (prop. 1997/98: 44 s. 101 f.). Förslaget i propositionen omfattade befogenheter som tillsynsmyndigheten bör ha och som enligt regeringen måste eller bör meddelas i lag. Regeringen anförde vidare att syftet med myndighetens tillsyn och rättigheter i samband med den är ytterst att myndigheten ska kunna konstatera om den behandling av personuppgifter som utförs är laglig. Kan myndigheten inte på begäran få tillgång till ett tillräckligt underlag för att konstatera att en behandling är laglig, bör myndigheten kunna vid vite förbjuda den personuppgiftsansvarige att fortsätta behandla personuppgifter på annat sätt än genom att lagra dem. Den som obstruerar riskerar således att bli förbjuden att i fortsättningen behandla personuppgifter. Om tillsynsmyndigheten får reda på att personuppgifter behandlas på ett olagligt sätt, bör enligt regeringen myndigheten i första hand försöka att åstadkomma rättelse genom påpekanden eller liknande förfaranden. Myndigheten bör dock kunna vid vite förbjuda den personuppgiftsansvarige att fortsätta att behandla personuppgifter på annat sätt än genom att lagra dem, om det inte går att få rättelse på annat sätt. Om saken är brådskande, bör myndigheten genast kunna gripa in på detta sätt. När det gällde myndighetens föreslagna befogenhet att få fatta ett tillfälligt beslut om vite, dvs. innan den personuppgiftsansvarige hade fått yttra sig, anförde regeringen att denna möjlighet endast borde utnyttjas när saken är klar och så brådskande att yttrandet inte kan avvaktas. I fråga om myndighetens möjlighet att hos förvaltningsrätt ansöka om utplånade av personuppgifter låg det enligt regeringen i sakens natur att möjligheten endast borde användas i sådana fall då

det inte genom andra åtgärder är möjligt att förena behandlingen av uppgifterna med de regler som gäller.

Förslag till uppgiftsskyddsförordning

Kommissionen

I likhet med dataskyddsdirektivet innehåller kommissionens förslag till uppgiftsskyddsförordning ett krav på varje medlemsstat att utse en eller flera offentliga myndigheter som ska vara ansvariga för att övervaka tillämpningen av förordningen (artikel 46.1). Om det finns flera tillsynsmyndigheter ska medlemsstaten utse den tillsynsmyndighet som ska fungera som enda kontaktpunkt så att myndigheten i fråga kan effektivt delta i Europeiska dataskyddsstyrelsens arbete (artikel 46.2).

I artikel 47.1 föreskrivs att tillsynsmyndigheten ska vara fullständigt oberoende i utövandet av det uppdrag och de befogenheter som den anförtrotts. Vidare ställs i artiklarna 47.2–42.7 ytterligare krav på medlemsstaterna som syftar till att säkerställa oberoendet hos tillsynsmyndighetens ledamöter och att myndigheten förfogar över egna resurser i form av bl.a. lokaler, personal och egen budget.

Enligt artikel 48.1 ska varje medlemsstat fastställa att tillsynsmyndighetens ledamöter ska utses antingen av medlemsstatens parlament eller av dess regering. I artiklarna 48.2–48.5 finns bestämmelser om villkor som gäller för ledamöternas uppdrag.

I artikel 49 finns regler för inrättandet av en tillsynsmyndighet, bl.a. att en sådan ska inrättas och att det ska fastställas vilka krav i fråga om kompetens, erfarenhet och sakkunskap som krävs för att utföra uppdraget som ledamot vid myndigheten.

I likhet med dataskyddsdirektivet finns krav på att tillsynsmyndighetens ledamöter och personal ska omfattas av tystnadsplikt (artikel 50).

Bestämmelser om tillsynsmyndighetens behörighet finns i artikel 51. Där sägs i 51.1 att varje myndighet ska inom sin medlemsstats territorium utöva de befogenheter som den tilldelas enligt förordningen. Enligt 51.2 ska i de fall en registeransvarig eller registerförare är etablerad i fler än en medlemsstat den tillsynsmyndighet, som är behörig på dess huvudsakliga verksamhetsställe, vara behörig att utöva tillsyn över all personuppgiftsbehandling som utförs av

denne registeransvarige i alla medlemsstater. Vidare sägs i artikel 51.3 att tillsynsmyndigheten inte ska vara behörig att utöva tillsyn över domstolar som behandlar personuppgifter som en del av sin dömande verksamhet.

I artikel 52 formuleras tillsynsmyndighetens uppdrag. Där sägs bl.a. att den ska övervaka och garantera tillämpningen av förordningen (punkt a), ta emot klagomål från registrerade, där så är lämpligt undersöka sakfrågan och inom rimlig tid underrätta den registrerade om hur behandlingen av klagomålet fortskrider och vilket slutsats som nås (punkt b), utföra undersökningar på eget initiativ, på grundval av klagomål eller på begäran av en annan tillsynsmyndighet (punkt d) samt följa sådan utveckling som påverkar skyddet av personuppgifter och bedriva rådgivningsverksamhet m.m. (punkterna e–j).

Enligt artikel 53.1 ska varje tillsynsmyndighet ha bl.a. följande befogenheter:

a) meddela den registeransvarige om att det finns en påstådd överträdelse av bestämmelserna om behandling av personuppgifter, och om så krävs specifikt beordra den registeransvarige att komma till rätta med överträdelsen,

b) beordra den registeransvarige att följa den registrerades krav att få utöva sina rättigheter enligt förordningen,

c) beordra den registeransvarige att lägga fram alla uppgifter som behövs för att myndigheten ska kunna fullgöra sitt uppdrag,

e) varna eller tillrättavisa den registeransvarige,

f) beordra rättelse, radering eller förstöring av alla uppgifter som har behandlats på ett sätt som står i strid med förordningen samt underrätta den tredje part till vilken uppgifterna har lämnats ut om dessa åtgärder,

g) tillfälligt eller definitivt förbjuda behandling,

h) avbryta flödet av uppgifter till en mottagare i tredje land eller en internationell organisation.

I artikel 53.2 föreskrivs att varje tillsynsmyndighet ska ha de undersökningsbefogenheter som behövs för att kräva följande av den registeransvarige:

a) tillgång till personuppgifter och all annan information som myndigheten behöver för att kunna fullgöra sitt uppdrag.

b) tillgång till den registeransvariges lokaler, inklusive all utrustning och alla andra medel för behandling av personuppgifter, om det finns rimliga skäl att anta att där har förekommit överträdelse av förordningen.

Befogenheterna i b ska utövas på ett sätt som är förenligt med unionens och medlemsstatens lagstiftning.

Tillsynsmyndighetens befogenheter enligt artikel 53.1 och 53.2 gäller även i förhållande till en registerförare.

Enligt artikel 53.3 ska varje tillsynsmyndighet ha befogenhet att upplysa de rättsliga myndigheterna om överträdelser av förordningen och att väcka talan vid domstol, särskilt enligt artiklarna 74.4 (föra talan på en registrerads vägnar mot en tillsynsmyndighet i en annan medlemsstat än den där den registrerade har sin hemvist, om den registrerade berörs av ett beslut av den myndigheten) och 75.2 (föra talan mot en registeransvarig eller registerförare).

Varje tillsynsmyndighet ska också ha befogenhet att utfärda sanktioner vid administrativa överträdelser, särskilt enligt artikel 79.4, 79.5 och 79.6. I dessa artiklar ges tillsynsmyndigheten befogenhet att utfärda böter till vissa fastställda belopp i förhållande till den registeransvarige vid olika former av överträdelser av förordningens bestämmelser.

I artikel 74.1 föreskrivs att varje fysisk eller juridisk person ska ha rätt till ett rättsmedel mot beslut som en tillsynsmyndighet har fattat med avseende på vederbörande. Vidare sägs i artikel 74.3 att talan mot ett beslut som fattats av en tillsynsmyndighet ska ges in vid domstolarna i den medlemsstat där myndigheten har sitt säte.

Europaparlamentet

I Europaparlamentets resolution med ändringsförslag föreslås bl.a. att artikel 51.1 ska ändras på så sätt att endast tillsynsmyndigheten i respektive medlemsstat ska vara behörig att utöva tillsyn över offentliga myndigheters behandling av personuppgifter. Dessutom föreslås att artikel 51.2 utgår.

Vidare föreslår parlamentet att det införs en ny punkt i artikel 52 (punkt 2a), där det bl.a. föreskrivs att alla tillsynsmyndigheter tillsammans med Europeiska dataskyddsstyrelsen ska föra ett register över sanktioner och överträdelser. Registret ska så detaljerat som möjligt innehålla alla varningar och sanktioner samt information om avhjälpande av överträdelser.

Parlamentet föreslår också att det i inledningen av artikel 53.1 skjuts in att varje tillsynsmyndighets befogenheter ska vara ”i linje med denna förordning” och alltså inte följa direkt av förordningen. I övrigt föreslås i princip inga ändringar av befogenheterna. Däremot anser parlamentet att det ska införas en ny punkt som innebär en befogenhet för varje tillsynsmyndighet att införa mekanismer för en s.k. visselblåsarfunktion.

Därutöver föreslår parlamentet att befogenheterna att utfärda sanktioner enligt artikel 53.4 ska avse hela artikel 79 samt att det ska läggas till att befogenheten ska utövas på ett effektivt, proportionellt och avskräckande sätt. Vad avser artikel 79 föreslås betydligt mer detaljerade bestämmelser än i kommissionens förslag om vilka faktorer som ska beaktas vid de administrativa sanktionerna.

Några kommentarer

Det kan konstateras att förslaget till uppgiftsskyddsförordning innehåller relativt stora skillnader i förhållande till dataskyddsdirektivet när det gäller en tillsynsmyndighets befogenheter. Det gäller inte minst i fråga om myndighetens behörighet att utöva sina befogenheter, eftersom den enligt kommissionens förslag till uppgiftsskyddsförordning utsträcks till att gälla också i fråga om uppgiftsbehandling i andra medlemsstater. En annan skillnad är att tillsynsmyndigheten enligt förslaget till förordning uttryckligen ska sakna behörighet att utöva tillsyn över domstolar när de behandlar personuppgifter som en del av sin dömande verksamhet.

När det gäller en tillsynsmyndighets befogenheter föreskrivs i dataskyddsdirektivet endast att myndigheten ska ha effektiva befogenheter att ingripa (artikel 28.3). Några tvingande regler om vilka befogenheter detta ska avse ges inte, utan i direktivet anges vissa exempel på effektiva befogenheter. I förslaget till uppgiftsskyddsförordning finns emellertid en uppräkning av vilka befogenheter

som myndigheten ska ha. Om dessa bestämmelser införs kommer alltså befogenheterna att följa direkt av förordningen och på motsvarande sätt gälla i förhållande till en myndighet som är registeransvarig. Europaparlamentets ändringförslag förefaller emellertid innebära att befogenheterna inte ska följa direkt av förordningen, de ska gälla ”i linje med förordningen”, vilket torde förutsätta att tillsynsmyndighetens befogenheter ges i nationell lagstiftning.

I artikel 28.3 i dataskyddsdirektivet sägs att varje tillsynsmyndighet ska ha undersökningsbefogenheter, varefter det som exempel på sådana befogenheter nämns att få tillgång till uppgifter som blir föremål för behandling och befogenhet att inhämta alla uppgifter som är nödvändiga för att sköta tillsynen. I artikel 53.2 förslaget till uppgiftsskyddsförordning ställs inte bara som krav att varje tillsynsmyndighet ska ha undersökningsbefogenheter, utan det föreskrivs också vad dessa ska bestå i.

I personuppgiftslagen har tillsynsmyndigheten getts befogenhet att i vissa fall besluta om vite i förhållande till den personuppgiftsansvarige. Denna befogenhet är inte någon följd av dataskyddsdirektivet, som saknar bestämmelser om att en tillsynsmyndighet ska kunna utfärda administrativa sanktioner. Förslaget till uppgiftsskyddsförordning ger emellertid tillsynsmyndigheterna befogenhet att besluta om administrativa sanktioner i form av böter till fastställda belopp eller, i fråga om företag, till viss procent av omsättningen. Några särskilda bestämmelser om administrativa sanktioner mot myndigheter föreslås inte, utan samma befogenheter avses gälla i förhållande till alla registeransvariga.

Av Europaparlamentets resolution med ändringsförslag framgår att parlamentet är i vissa delar emot att myndighetens behörighet utsträcks utanför den egna medlemsstaten. Exempelvis anser parlamentet att endast tillsynsmyndigheten i respektive medlemsstat ska vara behörig att utöva tillsyn över offentliga myndigheters behandling av uppgifter.

17.2 Reglering i registerförfattningar

Såvitt framgår av den inventering av registerförfattningarna som utredningen har genomfört torde det i princip inte förekomma att det har föreskrivits om undantag från Datainspektionens befogen-

het enligt 43 § PuL att på begäran få tillgång till de personuppgifter som behandlas, upplysningar om och dokumentation av behandlingen av personuppgifter och säkerheten vid denna samt tillträde till sådana lokaler som har anknytning till behandlingen av personuppgifter. Inspektionens befogenhet enligt personuppgiftslagen som syftar till att den ska kunna undersöka om personuppgifter behandlas på ett tillåtet sätt torde alltså gälla utan undantag över hela myndighetsområdet.

I allmänhet innehåller registerförfattningarna inte heller något undantag från 45 § första stycket första meningen PuL, där det föreskrivs att tillsynsmyndigheten ska genom påpekanden och eller liknande förfaranden försöka åstadkomma rättelse om personuppgifter behandlas eller kan komma att behandlas olagligt. Registerförfattningarna på skatteområdet och för Kronofogdemyndighetens verksamhet innehåller emellertid undantag från denna bestämmelses tillämpning. Som skäl anförde regeringen att det torde vara självklart att Datainspektionen vidtar de åtgärder som är rimliga för att få till stånd en rättelse när brister i myndigheternas hantering upptäcks (prop. 2000/01:33 s. 97).

När det gäller Datainspektionens befogenhet att vid vite förbjuda den personuppgiftsansvarige att behandla personuppgifter på annat sätt än genom att lagra dem – vilket kan bli aktuellt dels då inspektionen inte får tillräckligt underlag för att kunna konstatera om behandlingen är laglig efter en begäran enligt 43 § (44 §), dels då det inte går att få rättelse av en behandling som utförs eller kan komma att utföras på ett olagligt sätt eller saken är brådskande (45 § första stycket) – har undantag föreskrivits i en del registerförfattningar. Som exempel kan nämnas författningarna för Skatteverket och Tullverkets brottsbekämpande verksamhet samt Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst (ytterligare exempel nämns i Öman/Lindblom, s. 499). Som motivering har det ibland anförts att det inte kan anses behövligt att ha denna typ av bestämmelser, eftersom det får förutsättas att den berörda myndigheten och tillsynsmyndigheten har en dialog i en sådan fråga och att myndigheter följer tillsynsmyndighetens uppmaningar (prop. 2000/01:33 s. 96 och prop. 2006/07:46 s. 105). I andra fall har motiveringen varit att det följer av allmänna rättsgrundsatser att vite inte bör användas som sanktionsmedel mellan statliga myndigheter (prop. 2004/05:164 s. 54 och 2009/10:85 s. 90).

Som en följd av att Datainspektionen inte ska ha befogenhet att förbjuda viss behandling vid vite har undantag i förekommande fall även meddelats från en tillämpning av 46 § PuL, där det föreskrivs att den personuppgiftsansvarige dessförinnan ska få möjlighet att yttra sig och att vite i vissa fall ändå får meddelades om saken är brådskande.

I polisdatalagen (2010:361) har man skiljt på frågorna om Datainspektionens befogenhet att förbjuda annan behandling av personuppgifter än att lagra dem och att meddela sådant förbud vid vite (jfr 2 kap. 2 § första stycket 11 och fjärde stycket). Som skäl för att Datainspektionen ska ha befogenhet att förbjuda viss behandling anförde regeringen att sådana bestämmelser redan gällde inom polisens brottsbekämpande verksamhet och borde gälla även fortsättningsvis (prop. 2009/10:85 s. 90). Däremot borde av de ovan redovisade principiella skälen inte någon hänvisning göras till de bestämmelser i personuppgiftslagen som behandlar frågan om vite.

Även i promemorian med förslag till en ny domstolsdatalag har en motsvarande åtskillnad gjorts (Ds 2013:10 s. 161). Där konstateras emellertid att ett förbud för en domstol att behandla personuppgifter på något annat sätt än genom att lagra dem skulle i många fall innebära att verksamheten blockeras, vilket kan ha allvarliga följder för rättssäkerheten, tilltron till rättsväsendet och för enskildas möjligheter att ta tillvara sin rätt. Datainspektionen borde därför i det längsta undvika att tillgripa denna åtgärd. JO har i sitt remissvar över förslaget anfört, med hänvisning till de konsekvenser som det pekas på i promemorian, att Datainspektionen inte bör ha möjlighet att meddela denna typ av förbud (dnr R 26-2013).

I allmänhet brukar registerförfattningar inte innehålla något undantag från tillsynsmyndighetens befogenhet enligt 47 § PuL att hos förvaltningsrätten inom vars domkrets som tillsynsmyndigheten är belägen ansöka om att sådana personuppgifter som har behandlats på ett olagligt sätt ska utplånas.

17.3 Våra överväganden och förslag

17.3.1 Utgångspunkter för tillsynen på myndighetsområdet

Bedömning: Även om tillsynsmyndighetens nuvarande tillsynsuppgift inte har formulerats i någon författning, bör utgångspunkten vara att tillsynen över myndigheternas personuppgiftsbehandling ska fortgå såsom den hittills har bedrivits i praktiken, bl.a. genom att initieras via klagomål från enskilda eller genom att myndigheten agerar på eget initiativ.

Det finns också i fortsättningen ett stort behov av att olika berörda kontrollorgan samverkar när det gäller skyddet av personuppgifter.

Den rättsliga grunden för tillsynen

I lagstiftningsarbetet inför personuppgiftslagens införande synes frågan om dataskyddsdirektivets krav innebär att det behövs mer uttryckliga regler om vad som kan initiera Datainspektionens tillsyn, eller om det behövs av andra skäl, inte närmare ha berörts. I Datalagskommitténs betänkande berördes frågan enbart på så sätt att kommittén utgick från att Datainspektionen borde finnas kvar som en fristående myndighet och att inspektionen inte borde ha en utpräglad ombudsmannaverksamhet (SOU 1997:39 s. 448).

I 1 § förordningen (2007:975) med instruktion för Datainspektionen sägs att inspektionens uppgift är att verka för att människor skyddas mot att deras personliga integritet kränks genom behandling av personuppgifter och för att god sed iakttas i kreditupplysnings- och inkassoverksamhet. Vidare sägs att inspektionen särskilt ska inrikta sin verksamhet på att informera om gällande regler samt ge råd och hjälp åt personuppgiftsombud enligt personuppgiftslagen. Den ska också följa och beskriva utvecklingen på IT-området när det gäller frågor som rör integritet och ny teknik.

Några andra förordningsbestämmelser som allmänt rör Datainspektionens uppgifter och befogenheter i egenskap av tillsynsmyndighet enligt personuppgiftslagen synes inte ha införts. Det saknas således regler i svensk lagstiftning som exempelvis motsvarar artikel 28.4 där det sägs att var och en, på egen hand eller företrädd av

en organisation, kan vända sig till tillsynsmyndigheten med begäran om skydd för sina fri- och rättigheter med avseende på behandling av personuppgifter. Personen i fråga har enligt samma artikel en rätt att informeras om vilka följder hans begäran fått.

Instruktionen för Datainspektionen innehåller inte heller några bestämmelser om vad som kan initiera inspektionens tillsyn. Detta är däremot vanligt förekommande beträffande andra tillsynsmyndigheter. I exempelvis 26 kap. 2 § skollagen (2010:80) definieras Skolinspektionens tillsynsuppdrag såsom en självständig granskning som har till syfte att kontrollera om den verksamhet som granskas uppfyller de krav som följer av lagar och andra föreskrifter. I tillsynen ingår att fatta de beslut om åtgärder som kan behövas för att den huvudman som bedriver verksamheten ska rätta fel som upptäckts vid granskningen. Ett annat exempel är den tillsyn som Inspektionen för vård och omsorg bedriver enligt patientsäkerhetslagen (2010:659). I den lagen definieras vad tillsyn enligt lagen innebär (7 kap. 3 §). Lagen innehåller också bestämmelser som föreskriver att inspektionen ska efter anmälan pröva klagomål och att utredning också kan inledas på inspektionens eget initiativ (7 kap. 10–19 §§). Även hur JO:s tillsyn kan initieras regleras uttryckligen i 5 § lagen (1986:765) med instruktion för Riksdagens ombudsmän. I nämnda bestämmelse föreskrivs att ombudsmännens tillsyn bedrivs genom prövning av klagomål från allmänheten samt genom inspektioner och andra undersökningar, som ombudsmännen finner påkallade.

Att det inte finns några uttryckliga regler om vad som kan initiera ett tillsynsärende hos Datainspektionen synes emellertid i praktiken inte ha inneburit något problem, eftersom det förefaller vara allmänt accepterat att inspektionen har behörighet att besluta om en sådan åtgärd. På Datainspektionens webbplats ges upplysningen att inspektionen inte är skyldig att inleda en tillsyn p.g.a. klagomål som lämnas till den, utan att frågan om en tillsyn ska inledas avgörs självständigt av inspektionen. Det görs också klart att inspektionen inte agerar som ombud för den som klagar.

Förutom den ovan nämnda artikel 28.4 innehåller dataskyddsdirektivet inte några närmare bestämmelser om vad som kan initiera en tillsynsmyndighets tillsyn. I förslaget till uppgiftsskyddsförordning är denna fråga emellertid mer tydligt reglerad. I artikel 52.1 b föreskrivs i princip samma krav som ställs i artikel 28.4 i direktivet. Där sägs att tillsynsmyndigheten ska ansvara för att ta emot klago-

mål från registrerade, där så är lämpligt undersöka sakfrågan och inom rimlig tid underrätta den registrerade om hur behandlingen av klagomålet fortskrider och vilken slutsats som nås. Därtill föreskrivs i samma artikel att tillsynsmyndigheten ska ansvara för att utföra undersökningar på eget initiativ, på grundval av klagomål eller på begäran av en annan tillsynsmyndighet (punkten d).

Vi ser det inte som vår uppgift att överväga om det behöver införas några nya bestämmelser som tydliggör vad Datainspektionens tillsynsuppgift består i, exempelvis när det gäller skyldighet att ta emot och pröva klagomål från registrerade. Frågan har emellertid ett intresse för utredningen på så sätt att regler om vad som kan initiera Datainspektionens tillsyn påverkar inspektionens befogenheter i förhållande till myndigheter i deras egenskap av personuppgiftsansvariga.

Vi utgår således från att Datainspektionens tillsyn över myndigheternas behandling av personuppgifter tills vidare kommer att fortgå såsom den hittills har bedrivits i praktiken, dvs. att ett tillsynsärende initieras genom att inspektionen blir uppmärksammad på ett missförhållande genom ett klagomål eller genom att inspektionen av annat skäl beslutar att på eget initiativ inleda en granskning.

Vikten av att berörda kontrollorgan samverkar när det gäller skyddet av personuppgifter

Myndigheters automatiserade behandling av personuppgifter utgör i dag en integrerad del av myndigheternas verksamhet och därmed ett utflöde av den myndighetsutövning som myndigheterna ägnar sig åt. Det innebär att Datainspektionens tillsyn många gånger kan sammanfalla med eller nära ansluta till den tillsyn som JO bedriver utifrån ett mer övergripande verksamhetsperspektiv. JO:s tillsyn kan vidare rikta sig mot både myndigheten som sådan och enskilda tjänstemän, medan Datainspektionens tillsyn riktar sig enbart mot myndigheten i egenskap av personuppgiftsansvarig. Det innebär att JO utifrån sin tillsynsuppgift kan behandla frågor som rör skydd för personuppgifter från ett mer heltäckande perspektiv än vad Datainspektionen kan göra (se t.ex. JO:s beslut den 9 september 2014, dnr 3032-2011). JO kan också uttala sig i frågor om ansvar för att regler efterlevs inte bara på myndighetsnivå utan också i förhållande till enskilda tjänstemän. JO kan alltså både uttala sig om att myndigheten i något avseende inte har fullgjort sin uppgift som person-

uppgiftsansvarig och rikta kritik mot en enskild tjänsteman för en otillåten behandling som han eller hon har gjort sig skyldig till (se t.ex. JO:s beslut den 17 mars 2015, dnr 5205-2013). JO:s på detta sätt mer vidsträckta möjlighet att uttala sig om en otillåten hantering av personuppgifter får, vid sidan av Datainspektionens verksamhet, anses vara av stor vikt för att myndigheter ska få ledning i hur personuppgifter ska skyddas i deras verksamhet. Den lag som vi nu föreslår syftar visserligen till att reglerna för myndigheters behandling av personuppgifter ska vara enklare att tillämpa och stämma bättre överens med andra regelverk som styr myndigheters hantering av personuppgifter. Vi ser emellertid också i fortsättningen ett stort behov av ett väl fungerande samarbete mellan Datasinspektionen och JO.

Förutom JO har Justitiekanslern, JK, enligt lagen (1975:1339) om justitiekanslerns tillsyn ett allmänt uppdrag att ha tillsyn över att de som utövar offentlig verksamhet efterlever lagar och andra författningar samt i övrigt fullgör sina åligganden. Denna tillsyn omfattar både statliga myndigheter och anställda, uppdragstagare och andra som är knutna till sådana myndigheter som står under JK:s tillsyn. Under JK:s tillsyn står dessutom kommunala myndigheter och andra myndigheter som inte är statliga samt tjänstemän och befattningshavare vid sådana myndigheter. Även vissa andra befattningshavare som utövar myndighetsutövning i annan verksamhet m.m. omfattas av tillsynen. Inom ramen för denna tillsyn kan alltså JK få anledning att uttala sig om huruvida en viss myndighet uppfyller kraven i gällande bestämmelser i sin behandling av personuppgifter. Inom ramen för den frivilliga skaderegleringen på det statliga området ingår också i JK:s uppgifter att besluta om skadestånd i de fall en statlig myndighet har behandlat personuppgifter i strid med gällande bestämmelser. I dessa beslut gör således JK uttalanden om huruvida en viss behandling uppfyller kraven i gällande föreskrifter. Dessa beslut utgör således också viktig vägledning i frågor som rör myndigheters personuppgiftsbehandling.

17.3.2 Befogenheter för att undersöka om personuppgifter behandlas på ett tillåtet sätt

Förslag: I den nya lagen införs bestämmelser som ger tillsynsmyndigheten samma befogenheter som enligt gällande rätt att hos en myndighet undersöka om en behandling av personuppgifter sker i enlighet med de krav som gäller för verksamheten.

I personuppgiftslagen har Datainspektionen genom bestämmelserna i 43 § getts undersökningsbefogenheter som i princip motsvarar de krav som ställs i förslaget till uppgiftsskyddsförordning. Registerförfattningar brukar i allmänhet inte innehålla bestämmelser om att dessa befogenheter inte ska gälla på ett visst myndighetsområde. Enligt nuvarande bestämmelser torde befogenheterna alltså gälla fullt ut vid tillsyn hos alla myndigheter. Vi ser inte några skäl till att detta förhållande skulle behöva ändras. Tillsynsmyndigheten bör alltså även framöver ha samma befogenheter som i dag att hos en myndighet undersöka om en behandling av personuppgifter sker i enlighet med de krav som gäller för verksamheten.

17.3.3 Påpekanden eller andra åtgärder som inte är tvingande i förebyggande syfte

Förslag: Det ska framgå av den nya lagen att åtgärder från tillsynsmyndighetens sida i form påpekanden eller liknande förfaranden som inte har tvingande karaktär ska användas endast i förebyggande syfte och inte då det har konstaterats att en behandling av personuppgifter utförs på ett otillåtet sätt.

I förordningen (2007:975) med instruktion för Datainspektionen anges i 1 § att inspektionen ska särskilt inrikta sin verksamhet på att informera om gällande regler samt ge råd och hjälp åt personuppgiftsombud enligt personuppgiftslagen. Denna inriktning har även kommit till uttryck i personuppgiftslagens bestämmelser om tillsynsmyndighetens befogenheter. Av 45 § första stycket PuL följer således att tillsynsmyndigheten i första hand ska försöka åstadkomma rättelse genom påpekanden eller liknande förfaranden och att

detta gäller även om en behandling kan konstateras vara eller komma att bli olaglig.

Personuppgiftslagen anvisar alltså samma slags åtgärder från tillsynsmyndighetens sida oavsett om de avses användas i förebyggande syfte eller för att korrigera en behandling som konstaterats inte uppfylla lagens krav. Det har i praktiken bl.a. medfört att Datainspektionen – med stöd av 45 § första stycket PuL – har förelagt en personuppgiftsansvarig att åtgärda konstaterade brister i sin personuppgiftsbehandling. Genom den praxis som har utbildats kring tillsynsmyndighetens befogenheter enligt personuppgiftslagen får denna ordning anses ha accepterats (se t.ex. Kammarrätten i Stockholms dom den 6 mars 2013, mål nr 2415-12). I personuppgiftslagens mening ryms alltså en åtgärd från tillsynsmyndighetens sida i form av ett föreläggande inom ramen för uttrycket ”påpekanden och liknande förfaranden”. Denna tolkning ska emellertid ses i ljuset av att dels 45 § första stycket PuL också omfattar de fall då en behandling konstateras vara otillåten, dels att den tvingande åtgärd som enligt lagen annars står till buds är att förbjuda behandlingen.

I vissa fall då Datainspektionen konstaterat att en behandling inte uppfyller de krav som följer av de föreskrifter som gäller för den personuppgiftsansvariges verksamhet har det tidigare förekommit att inspektionen i sitt beslut, i stället för att förelägga vederbörande att åtgärda bristerna, uttalat att den personuppgiftsansvarige ”uppmanas ”att vidta vissa åtgärder eller att inspektionen ”förutsätter att” så sker. Det slaget av formuleringar från tillsynsmyndighetens sida har lett till oklarhet beträffande huruvida beslutet har sådana verkningar för den personuppgiftsansvarige eller andra att det är frågan om ett överklagbart beslut. I praxis har ett sådant beslut i sakligt hänseende ansetts ligga så nära ett formligt föreläggande att det har kunnat överklagas (se t.ex. Kammarrätten i Stockholms beslut den 23 januari 2001 i mål nr 1173-2001). Avgörande synes alltså vara den omständigheten att tillsynsmyndigheten konstaterar att en personuppgiftsbehandling inte uppfyller kraven i gällande föreskrifter även om den personuppgiftsansvarige trots det genom en inte tvingande formulering uppmanas att på eget initiativ komma till rätta med bristerna. Enligt vad vi har erfarit kan det finnas en risk för att ett sålunda utformat beslut kan uppfattas ha ett dubbelt och delvis motstridigt budskap och därför inte kommer att efterlevas.

Av artikel 12 b i dataskyddsdirektivet följer att medlemsstaterna ska säkerställa att varje registrerad har rätt att från den registeransvarige i förekommande fall få sådana uppgifter som inte behandlats i enlighet med direktivets bestämmelser korrigerade. Datainspektionens tillsynsuppgift innefattar visserligen efterlevnaden av hela lagstiftningen och inte enbart att korrigera en felaktig behandling av personuppgifter, dvs. även krav på exempelvis information och tillräckliga säkerhetsåtgärder. Enligt vår uppfattning synes det emellertid vara mer förenligt med kravet på att den registrerades rätt säkerställs och det grundläggande syftet med lagen att skydda enskildas personliga integritet att tillsynsmyndigheten genom någon form av påbud ingriper mot en personuppgiftsansvarig som brister i sina skyldigheter enligt lagen i stället för att anvisa denne att genom en frivillig åtgärd komma till rätta med bristerna.

Mot denna bakgrund anser vi att tillsynsmyndigheten inte bör använda sig av påpekanden och andra åtgärder som inte har en tvingande karaktär i de fall då myndigheten har konstaterat att en myndighet behandlar personuppgifter på ett sätt som inte uppfyller lagens krav. Denna typ av åtgärder, som alltså har karaktär av uppmaningar och inte påbud, bör endast användas i de fall det exempelvis finns en farhåga om att en behandling kan komma att ske på ett otillåtet sätt eller att det annars behövs för att förebygga att en behandling ska bli otillåten. Vi anser att detta bör komma till klart uttryck i den nya lagen och föreslår därför en bestämmelse med ett sådant innehåll.

17.3.4 Tvingande åtgärder i form av föreläggande eller förbud

Förslag: Tillsynsmyndigheten ska kunna förelägga en myndighet att uppfylla sina skyldigheter om myndigheten inte uppfyller de krav som följer av den nya lagen eller föreskrifter som meddelats med stöd av den. I föreläggandet ska anges vad tillsynsmyndigheten anser är nödvändigt för att avhjälpa de påtalade bristerna.

Tillsynsmyndigheten ska också ha befogenhet att förbjuda en myndighet att fortsätta en behandling av personuppgifter på något annat sätt än att uppgifterna lagras. Ett sådant beslut förutsätter att myndigheten allvarligt brister i sin skyldighet att uppfylla de krav som gäller för behandlingen.

Det är ett rimligt antagande att utgångspunkten är att myndigheter vill behandla personuppgifter på ett sätt som uppfyller de krav som gäller för myndigheten. Det finns emellertid exempel på att det kan uppstå situationer när Datainspektionen och myndigheten i fråga inte är överens om den aktuella behandlingen uppfyller kraven i gällande regelverk eller inte. I en sådan situation, dvs. då myndigheten inte själv har vidtagit åtgärder för att komma till rätta med brister som enligt tillsynsmyndigheten kan konstateras, är det likaså rimligt att tillsynsmyndigheten har mer kraftfulla maktmedel att ta till än att försöka åstadkomma rättelse genom påpekanden eller andra åtgärder som inte har en tvingande karaktär. Ett sådant ställningstagande förefaller vidare, som redan påpekats, vara mer förenligt med kravet på medlemsstaterna som följer av dataskyddsdirektivet att säkerställa den registrerades rätt att få en personuppgiftsbehandling som inte uppfyller direktivets krav korrigerad. Till bilden hör vidare att om artikel 53.1 i förslaget till uppgiftsskyddsförordning blir verklighet kommer en befogenhet för tillsynsmyndigheten att förbjuda behandling att följa direkt av förordningen.

Föreläggande att åtgärda en behandling som inte uppfyller gällande krav

Den praxis som utbildats rörande tillsynsmyndighetens nuvarande befogenheter enligt 45 § första stycket PuL kan sägas inrymma en möjlighet för Datainspektionen att förelägga en personuppgiftsansvarig att genom en viss påbjuden åtgärd komma till rätta med en otillåten behandling. En sådan möjlighet bör enligt vår uppfattning också följa av den nya lagen. Vi anser att den befogenheten emellertid bör komma till tydligare uttryck än vad som är fallet med formuleringen i 45 § första stycket PuL. Föreläggandet bör kunna ta sikte på samtliga skyldigheter som den personuppgiftsansvarige har enligt lagen eller föreskrifter som har meddelats med stöd av den. I den nya lagen bör det vidare ställas krav på att det av föreläggandet ska framgå vad inspektionen anser är nödvändigt för att påtalade brister ska avhjälpas.

Tillsynsmyndigheten ska alltså kunna använda sig av ett föreläggande i de fall där de konstaterade bristerna kan åtgärdas utan att det är nödvändigt att behandlingen som sådan upphör, såsom kan vara fallet om t.ex. ett visst register inte längre bör få föras. Som

exempel kan nämnas att personuppgifter som rör en viss registrerad har behandlats för länge på grund av att myndigheten i fråga om just dessa uppgifter inte har iakttagit de gallringsföreskrifter som gäller för behandlingen, vilken annars utförs för ett berättigat ändamål och även i övrigt uppfyller gällande krav. Ett annat exempel kan vara att myndigheten behöver vidta en viss säkerhetsåtgärd för att behandlingen ska kunna anses omgärdad av en tillräcklig säkerhetsnivå eller att två myndigheter har börjat utbyta personuppgifter genom direktåtkomst utan att träffa en sådan överenskommelse som vi föreslår ska krävas enligt den nya lagen (jfr kapitel 10).

Förbud mot att fortsätta en behandling

Det kan konstateras att Datainspektionens befogenhet enligt 44 och 45 §§ PuL att under vissa förutsättningar förbjuda annan behandling av personuppgifter än lagring kan få långtgående konsekvenser om ett sådant förbud meddelas för en myndighet. Såsom påpekades i promemorian med förslag till en ny domstolsdatalag skulle det i många fall innebära att verksamheten hindras helt och hållet (Ds 2013:10 s. 161). Det föranledde JO att i sitt remissvar avstyrka förslaget att Datainspektionen skulle ha möjlighet att meddela denna typ av förbud på domstolsområdet.

Det kan tyckas att domstolarna intar en särställning i samhället genom sin för rättssäkerheten principiellt viktiga uppgift såsom i många fall exklusiv utövare av makt i förhållande till enskilda och som den slutliga uttolkaren av en lagstiftnings innehåll. Men även vad gäller myndigheter i allmänhet torde det kunna konstateras att ett förbud att behandla personuppgifter på annat sätt än genom att lagra dem kan få allvarliga följder, inte bara för verksamhetens bedrivande som sådan utan även för enskildas möjligheter att i olika hänseenden tillvarata sina rättigheter liksom deras krav på service. Att myndigheters verksamhet kan hindras innebär därmed risker för den allmänna tilltron till det allmännas förmåga att bedriva samhällsnyttig verksamhet, vilket är allvarligt.

I vissa registerförfattningar har gjorts undantag från personuppgiftslagens nu aktuella bestämmelser på så sätt att Datainspektionen på myndighetsområdet i fråga inte har getts befogenhet att förbjuda en personuppgiftsbehandling. Utan att frågan har behandlats

särskilt utförligt i förarbetena får slutsatsen dras att i dessa lagstiftningsärenden har Datainspektionens möjlighet enligt 45 § första stycket att försöka åstadkomma rättelse genom påpekanden eller liknande förfaranden, dvs. inbegripet möjligheten att förelägga en myndighet att åtgärda en behandling som konstaterats brista i något avseende, samt befogenheten enligt 47 § att hos domstol ansöka om utplåning av uppgifter ansetts utgöra tillräckligt effektiva befogenheter.

Det kan mot den angivna bakgrunden ifrågasättas om tillsynsmyndigheten generellt sett alls bör ha en sådan långtgående befogenhet på myndighetsområdet och om så, om det bör införas bestämmelser som reglerar förutsättningarna för att meddela ett sådant förbud. Vårt förslag att tillsynsmyndigheten också enligt den nya lagen ska ha möjlighet att förelägga en myndighet att åtgärda brister i en viss personuppgiftsbehandling som myndigheten utför innebär att denna åtgärd bör vidtas då en iakttagen brist kan åtgärdas utan att behandlingen som sådan behöver upphöra. Men den situationen kan alltså uppstå att det förekommer sådana allvarliga brister ur integritetsskyddssynpunkt i samband med en viss personuppgiftsbehandling att behandlingen som sådan bör upphöra. Som exempel kan nämnas det s.k. Kringresanderegistret hos dåvarande Polismyndigheten i Skåne. Vid sin granskning fann Säkerhets- och integritetskyddsnämnden, SIN, att det förekommit generella och allvarliga brister vid polisens behandling av personuppgifter i registret, exempelvis att ändamålet med behandlingen var alldeles för vitt och att tillgången till personuppgifter i registret inte hade begränsats till varje tjänstemans behov (SIN:s uttalande den 15 november 2013, dnr 173-2013). Polismyndigheten beslutade därefter att avsluta registret (se SIN:s uttalande den 11 december 2014, dnr 463-2013). Ett annat exempel är Gotlands tingsrätts behandling av personuppgifter i form av att domstolens uppropslistor publicerades på domstolens webbplats. Datainspektionen konstaterade att publiceringen utgjorde en kränkning av registrerades personliga integritet enligt den s.k. missbruksregeln i 5 a § PuL och förelade tingsrätten att upphöra med publiceringen (beslut den 28 juni 2012, dnr 655-2012, se HFD 2014 ref. 32).

Som vi ser det kan man, sett till förvaltningsmyndigheters verksamhet i stort, alltså knappast utesluta att situationer kan uppstå där behovet av verksamma åtgärder i syfte att kunna avbryta pågå-

ende kränkningar av enskildas integritet är sådant att tillsynsmyndigheten måste ha befogenhet att kunna stoppa pågående behandlingar. Det går alltså inte att utesluta att det kan behövas en befogenhet för tillsynsmyndigheten att stoppa en pågående behandling även såvitt avser myndigheter. Däremot bör det gälla särskilda förutsättningar för ett ingripande av det slaget. Enligt vår mening bör tillsynsmyndigheten få ingripa genom ett förbud mot en fortsatt behandling av personuppgifter bara då en myndighet på ett allvarligt sätt har åsidosatt sina skyldigheter som personuppgiftsansvarig enligt den nya lagen och bristerna är av sådant slag att de inte kan åtgärdas på så sätt att ett tillräckligt skydd för personuppgifterna uppnås annat än genom att den aktuella behandlingen upphör. Det ska alltså exempelvis vara frågan om att en myndighet i en inte obetydlig omfattning behandlar känsliga personuppgifter trots att myndigheten saknar författningsstöd för det. Ett annat exempel kan vara att en myndighet har medgett en aktör direktåtkomst till sekretessreglerade personuppgifter trots att myndigheten saknar stöd för det i lag eller förordning. Att en myndighet på ett allvarligt sätt åsidosätter sin skyldighet att vidta åtgärder för att upprätthålla en tillräckligt hög säkerhetsnivå för en stor mängd känsliga personuppgifter är ytterligare exempel på en situation då tillsynsmyndigheten bör ha befogenhet att kunna förbjuda en fortsatt behandling.

Trots att myndigheten förbjuds att fortsätta en viss behandling av personuppgifter bör den ändå inte vara förhindrad att behandla uppgifterna genom att i någon form lagra dem, exempelvis för att det kan vara nödvändigt för att i ett senare skede kunna använda informationen som bevismedel i ett eventuellt skadeståndsärende. Detta bör framgå uttryckligen av den bestämmelse som vi nu föreslår.

17.3.5 Befogenhet att besluta om vite

Bedömning: Tillsynsmyndigheten bör inte ha befogenhet att rikta vitesföreläggande mot vare sig statliga eller kommunala myndigheter vars behandling av personuppgifter regleras av den nya lagen. Någon sådan bestämmelse föreslås därför inte.

Allmänt om viten på det offentligrättsliga området

Enligt 2 § lagen (1985:206) om viten, viteslagen, ska ett vitesföreläggande vara riktat till en eller flera namngivna fysiska eller juridiska personer. Det förefaller inte vara möjligt att utifrån rådande praxis på området få ett heltäckande svar på frågan om ett vite kan riktas till ett offentligrättsligt juridiskt objekt. Frågan behandlas utförligt i kommentaren till viteslagen (Lavin, Viteslagstiftningen, augusti 2010, Zeteo, kommentaren till 2 § viteslagen). Där redovisas bl.a. följande. Det finns författningsbestämmelser som innehåller uttryckliga förbud mot att vite föreläggs staten eller en kommun (se t.ex. 9 kap. 8 § andra stycket RB, ”staten” och 18 kap. 27 § fastighetstaxeringslagen [1979:1152], ”staten, kommun eller tjänsteman i tjänsten”). Socialstyrelsen har emellertid rätt att meddela vissa vitesförelägganden mot den som bedriver verksamhet enligt socialtjänstlagen (2001:453) och lagen (1993: 387) om stöd och service till vissa funktionshindrade, vilket kan vara en kommun. I den mån uttryckliga regler saknas, är rättsläget alltså oklart beträffande i vilken utsträckning ett vitesföreläggande kan, eller bör, riktas mot en offentligrättslig juridisk person. Det förekommer dock i praxis att viteshot har riktats mot en kommun och inte bara då den uppträtt som privaträttsligt subjekt. Det är däremot omöjligt att säga något bestämt om huruvida staten, då främst närmast ansvarig statlig myndighet, utan särskilt lagstöd kan vara adressat i ett vitesföreläggande. Den omständigheten att staten i princip betraktas som ett enhetligt rättssubjekt borde principiellt sett innebära att vitesförelägganden inte ska förekomma inom statlig offentlig verksamhet. Mer problematiskt är det fall då staten uppträder som privaträttsligt subjekt, t.ex. som arbetsgivare. Vidare kan eventuellt statliga affärsdrivande verk exempelvis kunna bli föremål för ett vitesföreläggande, eftersom verksamheten inte skiljer sig nämnvärt från den som bedrivs i ett statligt aktiebolag.

Enligt 4 kap. 5 § diskrimineringslagen (2008:567) kan ett vitesföreläggande riktas även mot staten som arbetsgivare när den inte fullgör sin skyldighet att vidta aktiva åtgärder enligt vad som föreskrivs i 3 kap. samma lag. Bestämmelsen motsvarar 35 § i den tidigare jämställdhetslagen (1991:433). I samband med att den bestämmelsen infördes erinrade Lagrådet om uttalandena i förarbetena till viteslagen (prop. 1984/85:96 s. 100) att det krävs att ett helt speciellt

undantagsfall är för handen för att vitesföreläggande mot staten ska komma i fråga (prop. 1999/2000:143 s. 156). Enligt Lagrådet hade det i lagrådsremissen inte anförts några bärande skäl för att denna mycket restriktiva inställning till att förelägga staten vite ska frångås just på jämställdhetsområdet. Regeringen delade emellertid inte Lagrådets bedömning utan ansåg att frågorna om jämställdhet och mångfald i arbetslivet är av sådan vikt att denna allmänt restriktiva inställning nu borde frångås (a. prop. s. 98 f.).

Även i arbetsmiljölagen (1977:1160) har det införts en möjlighet att rikta vitesförelägganden mot staten som arbetsgivare (7 kap. 7 § andra stycket). I förarbetena anförde regeringen att frågan om effektiva sanktioner för att förebygga skador och ohälsa i arbetslivet även på arbetsmiljö- och arbetstidsområdet är av sådan vikt att den restriktiva inställningen till att förelägga staten vid vite bör frångås (prop. 2012/13:143 s. 66 f.).

I sammanhanget kan noteras att Skolinspektionen har befogenhet enligt skollagen (2010:800) att rikta vitesföreläggande mot den som bedriver sådan verksamhet som står under inspektionens tillsyn, vilket kan vara både kommuner och enskilda. Vidare följer det av 21 § andra stycket lagen (1986:765) med instruktionen för Riksdagens ombudsmän att JO får förelägga vite om högst 10 000 kr när ombudsman inom ramen för sin tillsyn begär upplysningar och yttranden som domstolar, förvaltningsmyndigheter samt anställda hos staten eller kommun eller annan som står under en ombudsmans tillsyn är skyldiga att lämna enligt 13 kap. 6 § andra stycket RF. Det gäller emellertid inte i de ärenden där en ombudsman har beslutat om förundersökning.

Bör befogenheten att besluta om viten som riktas mot myndigheter finnas kvar?

Vid personuppgiftslagens införande fördes i förarbetena inga principiella resonemang angående den omständigheten att lagförslaget innehöll föreskrifter som gav Datainspektionen befogenhet att rikta vitesförbud även mot myndigheter, både statliga och kommunala, såsom personuppgiftsansvariga. Resonemangen rörde endast frågor om behovet av ett vitessanktionerat förbud och förutsättningar för att vitet skulle kunna dömas ut (prop. 1997/98:44 s. 102 f.). Någon remissinstans framförde synpunkten att ett förbud borde kunna

föregås av ett med vite förenat föreläggande för att uppnå det resultat som önskas. Enligt regeringens mening var det emellertid viktigt att tillsynsmyndigheten i första hand kunde fungera som ett stöd vid de personuppgiftsansvarigas behandling av personuppgifter och ge råd om hur behandlingen bör gå till för att vara laglig. Möjligheten till ett vitessanktionerat förbud fick anses tillräckligt för att förmå de personuppgiftsansvariga att följa tillsynsmyndighetens råd.

Som framgått har det i flera registerförfattningar som reglerar behandling av personuppgifter vid statliga myndigheter införts bestämmelser som föreskriver att Datainspektionens befogenhet enligt personuppgiftslagen att besluta om vite inte ska gälla i samband med tillsyn över den aktuella myndigheten. Som skäl har anförts att det följer av allmänna rättsgrundsatser att vite inte bör användas som sanktionsmedel mellan statliga myndigheter.

Av redovisningen ovan framgår alltså att det förekommer att viten kan riktas mot kommunala myndigheter, inte bara i de fall då de uppträder som ett privaträttsligt subjekt och även om det inte finns en uttrycklig bestämmelse som ger tillsynsmyndigheten i fråga en sådan befogenhet. Att en statlig tillsynsmyndighet kan rikta ett vite mot en annan statlig myndighet har emellertid ansetts strida mot allmänna rättsgrundsatser. Något uttryckligt förbud mot att rikta ett vite mot staten finns emellertid inte och från senare tid finns alltså ett par exempel på att lagstiftaren har frångått denna restriktiva inställning.

Datainspektionens nuvarande befogenhet att besluta om vite mot både staten och kommuner aktualiserar enligt vår mening återigen frågan om myndigheters behandling av personuppgifter ska ses som en verksamhet som innebär att myndigheter såsom personuppgiftsansvariga ska jämställas med privaträttsliga subjekt såvitt avser sådana skyldigheter som personuppgiftsansvaret innebär eller medför. Behandling av personuppgifter är visserligen i sig en verksamhet som kan bedrivas av både enskilda och det allmänna. Den behandling av personuppgifter hos myndigheter som den generella lagen avser att träffa sker emellertid uteslutande inom ramen för ett offentligrättsligt uppdrag. På det statliga området bedrivs denna verksamhet exklusivt av statliga myndigheter. Därmed finns enligt vår mening principiellt sett inget behov av att jämställa statliga myndigheters behandling av personuppgifter med enskilda aktörers behandling i

så måtto att samma villkor i alla delar bör gälla. Bilden är delvis annorlunda när det gäller det kommunala området, där t.ex. verksamhet inom den kommunala socialtjänsten och hälso- och sjukvården också bedrivs av enskilda. På skolområdet finns aktörer som fristående från såväl stat som kommun bedriver både grund- och gymnasieskola.

Enligt vår uppfattning innebär statliga myndigheters behandling av personuppgifter, som är en integrerad del i en myndighets hela verksamhet och myndighetsutövning, inte på något sätt att myndigheter kan anses agera på en marknad eller av annat skäl bör jämställas med eller anses agera som ett privaträttsligt subjekt. Eftersom dessa myndigheters behandling av personuppgifter sker i en verksamhet som i allmänhet inte förekommer utanför det allmänna och som omgärdas av helt andra krav och regler än vad som annars är fallet finns inga bärande skäl för att i alla delar ha samma sanktionsmöjligheter mot både myndigheter och enskilda. Det finns därmed inget sådant starkt vägande skäl som talar för att myndigheters behandling av personuppgifter utgör ett sådant undantagsfall att man bör avvika från den allmänna rättsgrundsatsen att staten inte kan rikta viten mot sig själv. Vi föreslår därför att tillsynsmyndigheten inte ska ha befogenhet att rikta viten mot andra statliga myndigheter, vare sig i samband med föreläggande eller för att sanktionera ett förbud mot behandling.

Vår ovan uttalade principiella syn på vad myndigheters behandling av personuppgifter utgör, dvs. en integrerad del i myndigheters egentliga uppdrag och verksamhet vilket normalt saknar privaträttsliga inslag, talar enligt vår uppfattning för att tillsynsmyndigheten som huvudregel inte heller ska ha någon befogenhet på det kommunala området att rikta viten mot myndigheterna där. Vi är emellertid väl medvetna om att det inom viss kommunal verksamhet såsom socialtjänst och hälso- och sjukvård däremot finns starka skäl för att så långt som möjligt jämställa villkoren för kommunala respektive enskilda aktörer. När det gäller behandling av personuppgifter inom dessa områden finns emellertid särskilda författningar som reglerar verksamheten och som riktar sig till alla huvudmän oavsett om de är en kommunal myndighet eller en enskild aktör. Personuppgiftsansvariga inom dessa områden kommer därför inte att träffas av den lag som vi nu föreslår, utan tillsynsmyndighetens befogen-

heter i förhållande till dess aktörer framgår i stället av respektive specialförfattning.

Vi föreslår således att den nya lagen inte ska innehålla någon föreskrift som ger tillsynsmyndigheten befogenhet att rikta viten mot de myndigheter som ska behandla personuppgifter enligt lagen. Förutom de starka principiella skäl som talar för att denna befogenhet inte bör finnas, kan det också konstateras att Datainspektionen inte i något fall har använt sig av möjligheten att vid vite förbjuda en myndighet att fortsätta med en viss behandling. Vad som föreskrivs om vite i 44–46 §§ PuL ska alltså inte gälla enligt den nya lagen.

Vårt förslag innebär att inte heller befogenheten enligt 45 § andra stycket PuL att föreskriva vite om en myndighet inte frivilligt följer ett beslut om säkerhetsåtgärder enligt 32 § kommer att finnas i fortsättningen. Det kan sättas i fråga om 32 § över huvud taget behöver kunna tillämpas på myndighetsområdet längre, eftersom vi föreslår att tillsynsmyndigheten uttryckligen ska ha befogenhet att utfärda förelägganden som kan ta sikte på en personuppgiftsansvarigs alla skyldigheter enligt lagen eller anslutande föreskrifter. Om det uppstår ett behov för tillsynsmyndigheten att ålägga en myndighet att på visst sätt höja sin säkerhetsnivå för personuppgifter som den behandlar bör det alltså lika bra kunna ske i form av ett föreläggande som ett beslut enligt 32 §. Det finns därför inte längre något behov av att kunna tillämpa 32 § på myndighetsområdet. Vi har i avsnitt 10.2 behandlat frågan om en myndighets skyldigheter enligt 31 § PuL att vidta nödvändiga säkerhetsåtgärder och om det finns ett behov av att på myndighetsområdet fylla ut denna bestämmelse med kompletterande regler.

17.3.6 Befogenhet att ansöka hos allmän förvaltningsdomstol om utplåning av uppgifter

Förslag: Tillsynsmyndigheten ska också i fortsättningen kunna ansöka hos en förvaltningsrätt om utplåning av personuppgifter som behandlas olagligt hos en myndighet.

Registerförfattningar brukar inte, som framgått ovan, innehålla något undantag från tillsynsmyndighetens befogenhet enligt 47 § PuL att hos förvaltningsrätt ansöka om utplåning av personuppgifter som har behandlats på ett olagligt sätt.

I sammanhanget kan dock konstateras att Datainspektionen hittills aldrig har använt sig av möjligheten att ansöka hos förvaltningsrätt om att personuppgifter ska utplånas. På myndighetsområdet kan man vidare fråga sig på vilken grund en domstol ska kunna besluta om att en utplåning ska ske. Vi har redan i avsnitt 15.4.4 konstaterat att när det gäller personuppgifter som finns i allmänna handlingar torde en myndighet inte en sådan befogenhet enbart med stöd av personuppgiftslagen eller den nya lagen. För en sådan åtgärd bör därför krävas särskilt lagstöd och sådant finns endast i undantagsfall.

Vi ser å andra sidan inte heller något direkt hinder mot att tillsynsmyndigheten även i fortsättningen ska kunna ha denna befogenhet på såväl det statliga som kommunala myndighetsområdet. Det kan inte uteslutas att en sådan ansökan någon gång kan visa sig vara en ändamålsenlig åtgärd för att tillgodose intresset av att motverka kränkningar av enskildas integritet genom olaglig behandling av personuppgifter. Vi menar därför att det i nuläget inte är motiverat att avskaffa denna möjlighet. I vilken mån den i praktiken går att utnyttja på myndighetsområdet får klargöras i rättstillämpningen. Vårt förslag är alltså att tillsynsmyndigheten också i fortsättningen ska kunna ansöka om utplåning av olagligt behandlade personuppgifter.

18 Övriga bestämmelser

18.1 Skadestånd och straff

18.1.1 Allmänna dataskyddsrättsliga regler

Dataskyddsdirektivet

Skadestånd

Enligt artikel 22 i dataskyddsdirektivet ska medlemsstaterna föreskriva att var och en har rätt att föra talan inför domstol om sådana kränkningar av rättigheter som skyddas av den nationella lagstiftning som är tillämplig på ifrågavarande behandling. Denna rätt påverkar inte möjligheten att utnyttja något administrativt förfarande, t.ex. vid tillsynsmyndigheten, som kan användas innan ett ärende anhängiggörs hos en rättslig instans.

Av artikel 23.1 följer att medlemsstaterna ska föreskriva att var och en som lidit skada till följd av en otillåten behandling eller av någon annan åtgärd som är oförenlig med de nationella bestämmelser som antagits till följd av direktivet, har rätt till ersättning av den registeransvarige för den skada som han eller hon har lidit.

I artikel 23.2 föreskrivs att den registeransvarige kan helt eller delvis undgå detta ansvar om han bevisar att han inte är ansvarig för den händelse som orsakade skadan.

Krav på sanktioner

Medlemsstaterna ska enligt artikel 24 anta lämpliga bestämmelser för att säkerställa att direktivet genomförs fullständigt och ska särskilt besluta om de sanktioner som ska användas vid överträdelse av de bestämmelser som antagits för att genomföra direktivet.

Personuppgiftslagen

Skadestånd

Enligt 48 § första stycket PuL ska den personuppgiftsansvarige ersätta den registrerade för skada och kränkning av den personliga integriteten som en behandling av personuppgifter i strid med denna lag har orsakat.

Vidare sägs i andra stycket att ersättningsskyldigheten kan jämkas i den utsträckning det är skäligt, om den personuppgiftsansvarige visar att felet inte berodde på honom eller henne.

I förarbetena till personuppgiftslagen anfördes att rätten till personlig integritet är en immateriell rättighet (prop. 1997/98:44 s. 106 f.). Någon ekonomisk skada behöver alltså inte uppstå vid en kränkning. Den enskilde, som drabbas av en olaglig behandling, bör därför ha rätt till ekonomisk kompensation för själva kränkningen förutom rätt till ersättning för personskada, sakskada och ren förmögenhetsskada. Alla åtgärder som är oförenliga med bestämmelserna i lagen kan leda till skadeståndsskyldighet. Skyldigheten är således mer vidsträckt än enligt den tidigare datalagen, där ersättningsansvaret var begränsat till oriktiga eller missvisande uppgifter eller vissa brott enligt den lagen. Den personuppgiftsansvarige är gentemot den registrerade ansvarig för all behandling som han eller hon har ansvaret för, även när ett personuppgiftsbiträde eller annan hjälp anlitas (a. prop. s. 144).

Skadeståndsansvaret enligt 48 § PuL är i princip strikt. Det krävs alltså inte att den personuppgiftsansvarige har haft uppsåt att skada någon eller att en otillåten behandling skett av oaktsamhet. För skadeståndsansvar räcker det med att den personuppgiftsansvarige har utfört en behandling i strid med lagens bestämmelser.

Straff

I 49 § föreskrivs att till böter eller fängelse i högst sex månader, eller om brottet är grovt, till fängelse i högst två år döms den som uppsåtligen eller av grov oaktsamhet lämnar osann uppgift i vissa fall, behandlar känsliga personuppgifter eller uppgifter om lagöverträdelser i strid med 13–21 §§ eller 5 a § andra stycket, i vissa fall

brister i sin anmälningsskyldighet eller i visst fall överträder förbudet mot överföring av personuppgifter till tredje land.

När det gäller bestämmelsen om straff anförde regeringen i förarbetena till personuppgiftslagen (prop. 1997/98:44 s. 108 f.) att de huvudsakliga sanktionerna mot de personuppgiftsansvariga som inte följer den nya lagen är skadestånd och vite. Dessa sanktioner för brott mot lagen fick anses effektiva och i stort sett tillräckliga. Det fanns emellertid behov av att kriminalisera vissa olagliga åtgärder. När personuppgiftslagen infördes omfattade straffbestämmelsen även överträdelser som begicks av oaktsamhet utan att de var grova. Genom lagändringar år 2006 avkriminaliserades oaktsamhet av normalgraden. I förarbetena anfördes som skäl bl.a. att utvecklingen hade gått mot att straff inte är en nödvändig reaktion på överträdelser av personuppgiftslagen eller anslutande registerförfattningar (prop. 2005/06:173 s. 48).

Det förefaller som om det inte finns något exempel i rättspraxis på att en person har dömts för brott mot personuppgiftslagen för en överträdelse som denne gjort sig skyldig till i egenskap av anställd hos en myndighet.

Förslaget till uppgiftsskyddsförordning

Skadeståndsansvar

I kommissionens förslag till uppgiftsskyddsförordning föreskrivs i artikel 75.1 att varje fysisk person som anser att hans eller hennes rättigheter enligt förordningen har åsidosatts som en följd av att personuppgifter har behandlats i strid med förordningen ska ha rätt att begära domstolsprövning. I likhet med dataskyddsdirektivets bestämmelser ska denna rätt inte påverka tillgängliga administrativa rättsmedel.

Enligt artikel 75.2 ska talan mot en registeransvarig eller registerförare väckas vid domstolarna i den medlemsstat där den registeransvarige eller registerföraren är etablerad eller där den registrerade har hemvist. Det senare gäller emellertid inte om registerföraren är en offentlig myndighet som agerar inom ramen för sin myndighetsutövning.

Enligt artikel 77.1 ska varje person eller medlemsstat som har lidit skada till följd av en otillåten behandling av uppgifter eller något

annat handlande som är oförenligt med förordningen ha rätt till ersättning av den registeransvarige eller den registerförare som bär ansvaret för den uppkomna skadan.

I artikel 77.2 finns en bestämmelse om solidariskt betalningsansvar om fler än en registeransvarig eller registerförare har medverkat vid behandlingen av uppgifter.

Vidare sägs i artikel 77.3 att den registeransvarige eller registerföraren helt eller delvis kan undgå ansvar om vederbörande bevisar att denne inte är ansvarig för den händelse som orsakade skadan.

Krav på påföljder

Medlemsstaterna ska enligt artikel 78.1 föreskriva påföljder för överträdelser av bestämmelserna i förordningen och vidta de åtgärder som krävs för att se till att dessa påföljder tillämpas. Påföljderna ska vara effektiva, proportionella och avskräckande.

Europaparlamentets resolution

I Europaparlamentets resolution med ändringsförslag föreslås inga ändringar av betydelse i de nu aktuella artiklarna.

Några kommentarer

Förslaget till artikel 75 i uppgiftsskyddsförordningen om rätten att vid domstol föra talan om den registrerades rättigheter har åsidosatts bygger på artikel 22 i dataskyddsdirektivet. Förordningsbestämmelsen innehåller emellertid också en forumregel som ger registrerade rätt att välja en domstol i den medlemsstat där den registeransvarige är etablerad eller där den registrerade har hemvist.

Även bestämmelsen i artikel 77 i förslaget till uppgiftsskyddsförordning bygger på motsvarande artikel i dataskyddsdirektivet (artikel 23). Rättigheten utvidgas dock till att också avse registerförares ansvar när denne orsakat skada och föreskriver ett solidariskt skadeståndsansvar för gemensamma registeransvariga eller registerförare.

Av förslaget till förordning framgår inte om rättigheten enligt artikel 77 innebär att den registrerade kan välja att begära ersättning från den registeransvarige eller registerföraren. Om inte en sådan valmöjlighet finns, kan det befaras att förordningens förslag innebär en sämre möjlighet att få ersättning än enligt dagens system. Ersättningsbestämmelserna enligt direktivet innebär ju att den registeransvarige alltid är ansvarig även för de felaktiga behandlingar som registerföraren utför. Om den registrerade med förordningens förslag inte har en möjlighet att välja att begära ersättning från den registeransvarige innebär det att det först måste klargöras vem som är ersättningsansvarig för en viss behandling. Exempelvis skulle det kunna uppstå en situation där en registerförare gör gällande att denne gjort sig skyldig till en otillåten behandling på grund av otillräckliga eller otydliga instruktioner från den registeransvarige. Om en sådan situation uppstår kan det alltså eventuellt innebära att den registrerade måste föra två processer för att få ersättning.

Förslaget till artikel 78 i uppgiftsskyddsförordningen om krav på påföljder motsvarar i allt väsentligt artikel 24 i dataskyddsdirektivet.

18.1.2 Reglering i registerförfattningar

Skadestånd

I allmänhet brukar det i registerförfattningar hänvisas till att 48 § PuL om skadestånd gäller när personuppgifter behandlas enligt den aktuella författningen. Myndighetens skadeståndsansvar enligt den bestämmelsen omfattar därmed överträdelser som begås mot i första hand reglerna i registerförfattningen, men även mot personuppgiftslagens bestämmelser i den mån de också gäller för myndighetens behandling av personuppgifter.

I några registerförfattningar finns föreskrifter som innebär att t.ex. 28 § PuL om rättelse inte ska tillämpas, utan att frågan om rättelse regleras i någon annan författning, exempelvis i 26 § förvaltningslagen (1986:223). I sådana fall kan inte 48 § PuL användas som grund för att begära skadestånd.

Straff

I flera registerförfattningar förekommer det att en hänvisning görs till 49 § PuL om straff vid brott mot vissa bestämmelser i lagen. Ett sådant exempel är 1 kap. 2 § första stycket 9 lagen (2001:181) om behandling av uppgifter i Skatteverkets beskattningsverksamhet enligt vilken bestämmelsen om straff i 49 § PuL gäller när personuppgifter behandlas enligt lagen eller enligt andra föreskrifter i det ämne som regleras i lagen. Vid lagens införande anförde Lagrådet att 49 § PuL föreskriver ansvar för överträdelser av olika bestämmelser i den lagen (prop. 2000/01:33 s. 346). Enligt legalitetsprincipen kan paragrafen inte ges motsvarande tillämpning beträffande överträdelser av bestämmelser i de lagar som föreslogs i lagstiftningsärendet. Hänvisningen till 49 § PuL fick därför endast den innebörden att ansvar inträder i händelse av överträdelser av de paragrafer i personuppgiftslagen som i övrigt ska gälla och som är straffsanktionerade. Lagrådet kunde emellertid inte se att det fanns något behov av att införa separata straffbestämmelser i de föreslagna registerlagarna. Regeringen instämde i Lagrådets bedömning (a. prop. s. 97).

Det förekommer i vissa registerförfattningar att någon hänvisning inte görs till 49 § PuL om straffansvar. Ett sådant exempel är lagen (2005:787) om behandling av personuppgifter i Tullverkets brottsbekämpande verksamhet. I förarbetena till den lagen anfördes att det saknades behov av en hänvisning till 49 § PuL, eftersom personuppgiftslagens bestämmelser om behandling av känsliga personuppgifter och överföring till tredje land inte skulle tillämpas och straffbestämmelsen skulle därför urholkas (prop. 2004/05:164 s. 55). Det fanns inte heller något behov av att införa separata straffbestämmelser i den nya lagen.

Ett annat exempel är polisdatalagen (2010:361). I förarbetena till den lagen pekades också på att behandlingen av personuppgifter skulle utföras av personer anställda vid statliga myndigheter som redan omfattas av bestämmelser om tjänstefel m.m. i brottsbalken (prop. 2009/10:85 s. 91). Även reglerna om disciplinansvar för tjänsteförseelse enligt lagen (1994:260) om offentlig anställning borde enligt regeringen vägas in vid bedömningen av behovet av en regel om straffansvar. Motsvarande påpekande görs i promemorian med förslag till en ny domstolsdatalag, där det även erinras om att straff för

dataintrång enligt 4 kap. 9 § c brottsbalken kan ha betydelse i sammanhanget (Ds 2013:10 s. 168 f.).

18.1.3 Allmänna regler om skadestånd och straff på myndighetsområdet

Det allmännas ansvar enligt skadeståndslagen

Enligt 3 kap. 2 § SkL, ska staten eller en kommun ersätta personskada, sakskada eller ren förmögenhetsskada, som vållas genom fel eller försummelse vid myndighetsutövning i verksamhet för vars fullgörande staten eller kommunen svarar. Ersättningsskyldigheten omfattar även ideell skada på grund av att någon annan kränkts på det sätt som anges i 2 kap. 3 § genom fel eller försummelse vid sådan myndighetsutövning.

I 2 kap. 3 § SkL föreskrivs att den som allvarligt kränker någon annan genom brott som innefattar ett angrepp mot dennes person, frihet, frid eller ära ska ersätta den skada som kränkningen innebär. För att få ideellt skadestånd för att någons personliga integritet har kränkts, dvs. ersättning för en skada som inte har samband med personskada eller någon form av ekonomisk skada, krävs alltså att kränkningen har skett genom ett brott. Det krävs också att kränkningen är allvarlig.

Att ersättning för kränkning ska kunna utgå med stöd av 3 kap. 2 § SkL, jämförd med 2 kap. 3 § samma lag, förutsätter att aktuella åtgärder från myndighetens sida har skett i samband med myndighetsutövning. Om det inte är fråga om myndighetsutövning kan skadestånd ändå utgå med stöd av 3 kap. 1 § SkL enligt reglerna om ansvar för skada som vållas av arbetstagare. En förutsättning för det är att kränkningen har orsakats av att den anställde har begått brott i tjänsten.

Genom Högsta domstolens praxis har det under senare tid lagts fast att det finns en rätt till ideellt skadestånd vid kränkningar av Europakonventionen i andra fall än de som regleras av skadeståndslagen. Det har bl.a. rört kränkningar av rätten till privat- och familjeliv enligt artikel 8 i konventionen. Utredningen om det allmännas ansvar enligt Europakonventionen föreslog i betänkandet Skadestånd och Europakonventionen (SOU 2010:87) att det ska införas en ny regel i skadeståndslagen som ger möjlighet för enskilda fysiska och

juridiska personer att få skadestånd av staten eller en kommun vid överträdelser av Europakonventionen. Förslaget har ännu inte lett till lagstiftning.

En enskild som anser att han eller hon har orsakats skada av det allmänna kan ansöka hos allmän domstol om stämning mot staten eller en kommun. Saken blir då prövad i den ordning som gäller för tvistemål.

I de fall det är fråga om en skada som orsakats av staten finns också en annan möjlighet. Justitiekanslern, JK, kan besluta om skadestånd till enskilda inom ramen för statens frivilliga skadereglering. Sådana anspråk från enskilda handläggs enligt förordningen (1995:1301) om handläggning av skadeståndsanspråk mot staten. Det kan handla om anspråk som bl.a. grundas på 3 kap. 1–2 §§ SkL eller 48 § PuL. Denna skadereglering är kostnadsfri för den enskilde. Även viss ersättning för ombudskostnader kan utgå. Om man inte är nöjd med JK:s beslut kan man föra talan på sedvanligt sätt inför domstol.

Enligt 10 § förordningen om handläggning av skadeståndsanspråk mot staten får JK uppdra åt annan myndighet att fullgöra de uppgifter som JK har enligt förordningen. Ett sådant uppdrag har getts åt Skatteverket. Det innebär att Skatteverket bl.a. får handlägga skadeståndsanspråk mot staten som grundas på uppenbara registerskador hänförliga till behandlingen av personuppgifter i register för vilka Skatteverket ansvarar enligt personuppgiftslagen och där ersättningsbeloppet uppgår till högst 5 000 kr.

Några motsvarande bestämmelser som rör frivillig skadereglering på det kommunala området finns inte. Det står emellertid en kommun fritt att själv reglera en skada som en enskild orsakats inom ramen för kommunens verksamhet, exempelvis i samband med en otillåten behandling av personuppgifter. Såvitt utredningen har erfarit har sådan frivillig skadeståndsreglering ägt rum inom ett landsting eller en kommun i endast ett fåtal fall. Om ett landsting eller en kommun inte själv vill reglera en skada, får den enskilde alltså vända sig till allmän domstol. Sedan den 1 juli 2014 är ansökningsavgiften i allmän domstol 900 kr i ett mål där värdet av vad som yrkas inte uppgår till mer än ett halvt prisbasbelopp och annars 2 800 kr.

Straffbestämmelser m.m. på myndighetsområdet

Ett brott som på myndighetsområdet kan förorsaka en sådan kränkning som kan föranleda skadeståndsansvar enligt 2 kap. 3 § SkL är tjänstefel enligt 20 kap. 1 § BrB.

När det gäller andra brott som kan ha samband med en otillåten hantering av personuppgifter kan även brott mot tystnadsplikt enligt 20 kap. 3 § BrB komma i fråga. Detsamma gäller brottet dataintrång enligt 4 kap. 9 c § BrB.

I sammanhanget kan också nämnas bestämmelserna om disciplinansvar i lagen (1994:260) om offentlig anställning. Enligt dessa bestämmelser kan en arbetstagare meddelas disciplinpåföljd för tjänsteförseelse i form av varning eller löneavdrag. För detta gäller dock vissa förutsättningar, bl.a. att den misstänkta gärningen inte ska anmälas till åtal eller, om gärningen prövats i straffrättslig ordning, inte har ansetts vara något brott p.g.a. någon annan anledning än bristande bevisning. Genom Arbetsdomstolens praxis har bl.a. prövats frågan om disciplinansvar för en handläggare som gjort obehöriga sökningar i Försäkringskassans datasystem (AD 2005:82).

18.1.4 Justitiekanslerns skadereglering på grund av 48 § personuppgiftslagen

Allmänt om verksamheten

Sedan personuppgiftlagen trädde i kraft har JK inom ramen för statens frivilliga skadereglering handlagt ärenden som rör skadeståndsanspråk enligt 48 § PuL. Under åren 2011–2013 kom det in 196 sådana ärenden. Under samma period avgjorde JK 225 ärenden varav ersättning utgick i 131 fall, dvs. i ca 60 procent av ärendena. Denna andel kan jämföras med att det i ett ärende om skadeståndsanspråk mot staten som grundas på skadeståndslagen normalt utgår ersättning i 12–13 procent av ärendena. Som exempel på skador på grund av överträdelse av personuppgiftslagen som enligt JK:s beslut medfört ersättningsskyldighet kan nämnas bristande gallringsrutiner och felaktiga personuppgifter i olika register, exempelvis avseende folkbokföringen och hos Försäkringskassan.

Den 1 januari 2015 hade det kommit in ca 2 900 ärenden som rör det s.k. Kringresanderegistret som förts av dåvarande Polismyndig-

heten i Skåne (se vidare nedan om JK:s beslut den 7 maj 2014). Ytterligare sådana ärenden kommer fortfarande in till myndigheten.

Exempel från Justitiekanslerns skadereglering

Förutsättningar för att ersättning alls ska utgå

I ett beslut från den 2 mars 2011 (dnr 8156-09-40) uttalade JK vilka omständigheter som bör beaktas för att det alls ska finnas en rätt till ersättning enligt 48 § PuL. Av beslutet kan utläsas att det enligt JK inte räcker med att skadeståndskyldighet i och för sig föreligger, dvs. att en behandling har skett i strid med lagen, för att också ersättning ska utgå. I sak gällde beslutet om skadestånd enligt 48 § PuL skulle utgå med anledning av bl.a. ett felaktigt beslut om sjukpenning. JK fann att Försäkringskassans register under en tid kommit att innehålla en felaktig uppgift. Detta kom att påverka den aktuella personens sjukpenningförmåner och ledde senare till att vederbörande fick återbetala det som uppburits för mycket. Felet hade inneburit att en personuppgift hade hanterats i strid med 9 § g PuL, varför skadeståndsskyldighet för staten i och för sig hade uppkommit. Mot bakgrund av förarbetsuttalanden till den tidigare datalagen och de år 2002 ändrade reglerna om rätt till ersättning för ideell skada i skadeståndslagen fann JK att i princip samma omständigheter som ska beaktas när ersättning för kränkning bestäms bör ligga till grund för bedömningen av om det alls finns rätt till ersättning enligt 48 § PuL. Av betydelse är alltså om det har varit fråga om registrering av personuppgifter av känslig art, om det funnits risk för otillbörlig spridning av uppgifterna och om den felaktiga behandlingen fått eller kunnat få några beaktansvärda negativa konsekvenser för den registrerade. Om så inte är fallet kan en begäran om ersättning avslås även i de fall där en kränkning i och för sig anses ha skett, men bedöms vara försumbar. I det aktuella ärendet fann JK att den felaktiga behandlingen av personuppgiften inte kunde ha orsakat någon sådan kränkning av den berörda personens personliga integritet som är en förutsättning för rätt till ersättning enligt personuppgiftslagen.

Ersättningsbeloppets storlek

I ett beslut den 7 maj 2014 (dnr 1441-14-47) prövade JK skadeståndsanspråk med hänvisning till att personuppgifter i det s.k. Kringresanderegistret hade behandlats i strid med polisdatalagen (2010:361). Säkerhets- och integritetsskyddsnämnden (SIN) hade den 15 november 2013 uttalat att behandlingen av personuppgifter hade brister på så sätt att ändamålet med behandlingen var för oprecist, tillgången till personuppgifterna inte var begränsade till varje tjänstemans behov och att ingen loggning hade förekommit när personuppgifter behandlats. SIN hade anmält till JK att de generella brister som förekommit vid polisens behandling av personuppgifter i registret, som omfattade drygt 4 700 personer, var sådana som kan medföra skadeståndsansvar för staten (jfr 20 § förordningen [2007:1141] med instruktion för Säkerhets- och integritetsskyddsnämnden). Många personer hade också begärt ersättning av staten, bl.a. genom att vända sig till JK.

JK instämde i SIN:s bedömning att polisens behandling av personuppgifter i Kringresanderegistret i flera avseenden stått i strid med lag. Mot bakgrund av att det var fråga om integritetskänsliga personuppgifter och att de generella bristerna i behandlingen av dem sammantaget var allvarliga måste de personer vilkas uppgifter behandlats i registret anses ha blivit utsatta för en sådan kränkning av den personliga integriteten att de var berättigade till ersättning av staten enligt 48 § PuL. Kränkningen kunde med hänsyn till registrets inriktning och syfte samt de brister som konstaterats inte anses som mindre allvarlig. De brister som förekommit i registret hade emellertid inte lett till några negativa beslut eller åtgärder som inte uppkommit om behandlingen skett helt i enlighet med polisdatalagens bestämmelser. Den som varit föremål för registrering i Kringresanderegistret borde därför vara berättigad till ersättning för kränkning med 5 000 kr. Vid bedömningen av ersättningsbeloppets storlek beaktade JK att Högsta domstolen slagit fast att en schabloniserad bedömning i stor utsträckning kunde användas då en kränkningsersättning ska bestämmas, eftersom det sker utifrån en bedömning av vilken kränkning som typiskt sett får anses ha uppkommit (NJA 2013 s. 1046). Ersättning för en kränkning som bedöms som mindre allvarlig bör enligt Högsta domstolen i normalfallet bestämmas till 3 000 kr.

Det kan noteras att dåvarande Polismyndigheten i Skånes brister i behandlingen av personuppgifter i det s.k. Kringresanderegistret sammantaget kan komma att kosta Polismyndigheten omkring 20 miljoner kr till följd av krav på ersättning från de registrerade.

Från JK:s praxis kan också nämnas två beslut där det bedömts att väsentligt högre ersättningsbelopp än vad som normalt är fallet skulle utgå. Det ena beslutet, från den 29 mars 2010 (dnr 8043-08-42), rörde en person för vilken det felaktigt hade registrerats i belastningsregistret att han var dömd av norsk domstol för försök till ett grovt brott. JK konstaterade att det tagit exceptionellt lång tid från det att uppgifterna rätteligen borde ha tagits bort ut registret till dess att så skedde, att det var fråga om uppgifter av mycket känslig art som var direkt felaktiga, att registreringen utgjorde ett obefogat ingrepp i personens privat- och familjeliv och att registreringen hade medfört att han tillfälligt förlorat sitt arbete. Vid en samlad bedömning bestämdes kränkningsersättningen till 25 000 kr.

Det andra beslutet, från den 14 oktober 2010 (dnr 1813-10-42), rörde en person som felaktigt hade registrerats som avliden hos Försäkringskassan och Pensionsmyndigheten. Enligt JK hade den felaktiga registreringen rört ett mycket integritetskänsligt område. Felet hade vidarebefordrats till premiepensionsregistret vilket hade förorsakat ytterligare problem och olägenheter. JK ansåg att personen i fråga hade orsakats ett betydande lidande. Han hade också under lång tid varit felaktigt registrerad som avliden. Skälig ersättning i detta fall uppgick till 30 000 kr. JK fann det vidare rimligt att Försäkringskassan, som orsakat felet, ansvarade för hela den skada som uppstått.

Fråga om ersättning skulle utgå på grund av publicering på publik respektive intern webbplats

I ett beslut den 24 januari 2005 (dnr 2370-04-42) prövade JK skadeståndsanspråk med anledning av att Kriminalvårdsstyrelsen hade gjort en dom från Arbetsdomstolen tillgänglig i fulltext på intranätet. Domen rörde en tvist mellan Kriminalvårdsstyrelsen och en anställd, vars namn hade ersatts av initialerna. Datainspektionen hade i ett tidigare beslut funnit att myndigheten behandlat känsliga personuppgifter i strid med personuppgiftslagen eftersom domen innehöll uppgifter om den anställdes hälsa. JK kom till samma slutsats. Den

berörda personen hade därför rätt till ersättning enligt 48 § PuL. Vid bedömningen av skadeståndsbeloppets storlek beaktade JK att uppgifterna rörde särskilt integritetskänsliga förhållanden, att uppgifterna funnits på intranätet i sju månader och varit tillgängliga för ca 8 000 användare, såväl de närmaste arbetskamraterna som andra anställda. Vidare beaktade JK den omständigheten att om Kriminalvårdsstyrelsen hade valt att enbart ha en länk till Arbetsdomstolens webbsida eller till Lagrummet hade detta inte varit i strid med personuppgiftslagen. Skadeståndet bestämdes till 15 000 kr.

Enligt JK:s beslut den 26 september 2007 (dnr 3497-06-40) skulle Rikspolisstyrelsen betala skadestånd till två personer med vardera 25 000 kr på grund av att kränkande uppgifter i en rapport från Rikskriminalpolisen hade lagts ut på myndighetens webbplats. Rapporten rörde nationella hot- och problembilder och framställdes med viss regelbundenhet för i princip internt bruk. Efter önskemål från framför allt medierna hade dock en sekretessprövad version gjorts tillgänglig på Rikspolisstyrelsens webbplats på internet. Rapporten innehöll ett avsnitt om hur hot, våld, utpressning och bestickning kan utgöra försök att påverka utgången i ett myndighetsärende. I det sammanhanget nämndes som exempel en bok som de i skadeståndsärendet berörda personerna skrivit som rörde deras kontakter med Skatteverket. JK uttalade att undantagen i 7 och 8 §§ PuL inte var aktuella samt att myndigheter inte kan åberopa meddelarfrihet. Vid en prövning av om publiceringen kunde utgöra en tillåten behandling av personuppgifter enligt 10 § f PuL, fann JK att det inte fanns något särskilt tungt vägande skäl att tillhandahålla de berörda personernas personuppgifter på det sätt som nu blivit fallet.

I ett beslut den 19 februari 2008 (dnr 805-08-40) fann JK att någon ersättning inte skulle utgå med anledning av ett skadeståndsanspråk som grundades på att en polismyndighet gjort en bildpublicering på internet. Publiceringen avsåg en film som spelats in av en övervakningskamera i en butik. Polisen valde att offentliggöra den för att få information om ett rånförsök som butiken utsatts för. Efter att filmen lagts ut på polisens hemsida hade en lokaltidning kopierat den och lagt ut den på sin hemsida. JK hade granskat ärendet tidigare i egenskap av tillsynsmyndighet och hade då kommit fram till att det varken i sekretesshänseende eller i övrigt fanns anledning att rikta kritik mot polisen på grund av offentliggörandet. I det nu aktuella skadeståndsärendet fann JK att det hade rört sig

om en kort filmsekvens där den berörda personen förekom under en mycket begränsad tid. Uppgifterna om hennes personliga förhållanden i filmen kunde inte anses vara av ömtåligt slag även om de i och för sig hade fått stor spridning. Polisens behandling av uppgifterna hade dock inte skett med något otillbörligt syfte utan för att försöka få information om ett brott. Det var därför inte fråga om en sådan kränkning av den berördas personliga integritet som avses i 5 a § PuL. Det förelåg inte heller på annan grund skadeståndsskyldighet enligt 48 § PuL.

Skadeståndsansvarets fördelning om flera statliga myndigheter är inblandade

I ett beslut den 3 mars 2009 (dnr 6961-08-40) prövade JK ett ersättningsanspråk som grundade sig på att en länsstyrelse felaktigt hade fört in i vägtrafikregistret att det för en person gällde villkor om glasögon för körkort. JK konstaterade att den felaktiga personuppgiften hade förts in i registret av länsstyrelsen, medan det var Vägverket som var personuppgiftsansvarig för registret. I en situation där det är en statlig myndighet som är personuppgiftsansvarig bör 48 § PuL enligt JK förstås så att det är staten som är ersättningsskyldig. För det fall flera enheter inom staten är berörda bör fördelningen av ansvaret dem emellan bli en fråga för staten själv. Därvid bör den principen tillämpas som innebär att ersättning ska utges av den enhet som bär huvudansvaret för felet. Det betydde i det aktuella fallet att länsstyrelsen skulle ombesörja att ersättning betalades ut till personen i fråga.

JK har i ett tidigare beslut (2006-09-12, dnr 1127-05-42) kommit till samma slutsats.

18.1.5 Våra överväganden och förslag

Förslag och bedömning: I den nya lagen införs en bestämmelse som innebär att 48 § PuL om skadestånd gäller vid behandling av personuppgifter enligt den nya lagen eller enligt föreskrifter som meddelats med stöd av lagen.

Straffbestämmelsen i 49 § PuL kan inte medföra straffansvar för överträdelser av bestämmelser i den nya lagen. Något behov av att införa särskilda straffbestämmelser i den lagen finns inte. Lagen ska inte heller hänvisa till 49 § PuL. Skadeståndssanktionen får anses tillräcklig på myndighetsområdet.

Skadestånd

Genom att skadeståndsbestämmelsen 48 § PuL i allmänhet också gäller på de myndighetsområden som har särreglerats genom en registerförfattning medför den ett skadeståndsansvar för de allra flesta myndigheter vid deras behandling av personuppgifter, dvs. oavsett om behandlingen regleras av personuppgiftslagen eller i en registerförfattning. Enligt dataskyddsdirektivet finns ingen möjlighet att ha regler som innebär att en viss otillåten behandling inte ska medföra skadeståndsansvar för den personuppgiftansvarige. Någon sådan möjlighet finns inte heller i förslaget till en uppgiftskyddsförordning. I den nya lagen om myndigheters behandling av personuppgifter behöver det därför finnas en skadeståndsbestämmelse som kan tillämpas vid alla former av otillåten behandling enligt lagen. Något behov av att införa en särskild sådan bestämmelse i lagen finns inte, utan en hänvisning till 48 § PuL bör göras. Vi föreslår därför att det av den nya lagen ska framgå att den bestämmelsen gäller när personuppgifter behandlas enligt den nya lagen eller enligt föreskrifter som har meddelats i anslutning till lagen. Enligt den nya lagen kommer alltså en myndighet att på samma sätt som tidigare ha ett skadeståndsansvar för en behandling av personuppgifter som den utför i strid med de bestämmelser som gäller för myndigheten.

Enligt förslaget till uppgiftsskyddsförordning ska det även finnas, till skillnad från i dataskyddsdirektivet, möjlighet att rikta en skadeståndstalan mot en registerförare, dvs. ett personuppgiftsbiträde. Det saknas enligt vår uppfattning tillräckliga skäl för att på myn-

dighetsområdet redan nu föra in en sådan nyordning. Inte heller den föreslagna bestämmelsen i förordningen som syftar till att klargöra att det gäller ett solidariskt betalningsansvar bör nu införas på myndighetsområdet. På området för statliga myndigheter sker redan en ansvarsfördelning utifrån rättsgrundsatsen att staten är ett enhetligt rättssubjekt. I de fall det är fråga om flera statliga myndigheter som är inblandade i en behandling av personuppgifter är det, som redovisats, inte nödvändigtvis den myndighet som är personuppgiftsansvarig som ska betala skadeståndsersättningen utan detta kan i stället ankomma på den myndighet som bär huvudansvaret för att en otillåten behandling ägt rum.

I vårt uppdrag ingår inte att överväga en ny ordning för på vilket sätt en registrerad ska kunna föra talan om skada och kränkningar som har sin grund i att en myndighet har behandlat personuppgifter på ett otillåtet sätt. Det kan emellertid konstateras att den frivilliga skadereglering som handläggs av JK enligt förordningen (1995:1301) om handläggning av skadeståndsanspråk mot staten utgör ett relativt lättillgängligt rättsmedel när det är fråga om statliga myndigheters behandling av personuppgifter, bl.a. eftersom det är kostnadsfritt. Detta till skillnad från vad som är fallet på det kommunala området där det enda faktiskt tillgängliga rättsmedlet är att stämma berörd kommun inför allmän domstol. Dataskyddsdirektivet ställer dock inte upp några krav på hur lätt tillgängligt ett rättsmedel för att föra skadeståndstalan ska vara, utan det krävs endast att var och en ska ha rätt att föra en talan inför domstol. I direktivets perspektiv uppfyller alltså de svenska reglerna de krav som ställs, även om rättsmedlen är utformade på olika sätt beroende på vem som är personuppgiftsansvarig.

Straff

Både dataskyddsdirektivet och förslaget till uppgiftsskyddsförordning innehåller bestämmelser som innebär att medlemsstaterna ska föreskriva sanktioner eller påföljder som ska säkerställa att bestämmelserna om skydd för personuppgifter i respektive regelverk inte överträds. Något uttryckligt krav på att det ska införas straffbestämmelser finns inte. Huruvida det ska finnas straffbestämmelser för överträdelser av de bestämmelser om skydd för personuppgifter som

gäller för svenska myndigheter är alltså en fråga som den svenske lagstiftaren själv råder över.

Till skillnad från vad som är fallet enligt skadeståndslagen är skadeståndsansvaret enligt personuppgiftslagen strikt och det gäller även för myndigheter. Det krävs alltså exempelvis inte att ett brott har begåtts av en anställd hos en myndighet för att ersättning för kränkning enligt 48 § PuL ska kunna utgå. Behovet av straffbestämmelser kan alltså bedömas utan att någon koppling behöver göras till möjligheten att få skadestånd för kränkning vid en otillåten behandling.

Bestämmelsen om straff i 49 § PuL tar sikte på överträdelser av sådana bestämmelser i den lagen som endera inte föreslås gälla för myndigheterna enligt den nya lagen eller som inte fullt ut föreskriver vad som i en viss fråga gäller för myndigheters behandling av personuppgifter. Så är exempelvis fallet med de föreslagna bestämmelserna om när en myndighet får behandla känsliga personuppgifter. Om en överträdelse av bestämmelserna för när en sådan behandling är tillåten ska vara straffsanktionerad, behöver det alltså införas separata straffbestämmelser i den nya lagen vid sidan av 49 § PuL. Det ligger i sakens natur att nya straffbestämmelser inte ska införas utan att det finns ett starkt behov av det.

Den nya lagen innehåller enbart bestämmelser som riktar sig till myndigheter som är personuppgiftsansvariga. Det finns ingen bestämmelse som föreskriver någon skyldighet för en anställd vid myndigheten, dvs. som riktar sig mot en enskild person. Det är således myndigheten som sådan i egenskap av personuppgiftsansvarig som svarar för att samtliga bestämmelser i lagen följs vid den behandling av personuppgifter som sker vid myndigheten. Redan denna omständighet i sig talar för att lagen inte bör innehålla några straffbestämmelser, eftersom en myndighet inte kan begå brott.

I samband med införandet av de registerförfattningar där man avstått från att införa separata straffbestämmelser har lagstiftaren i flera fall påpekat att anställda vid både statliga och kommunala myndigheter redan omfattas av vissa straffbestämmelser som kan medföra straffansvar då den anställde bryter mot regler som gäller på myndighetens område. Som exempel kan nämnas brotten tjänstefel, brott mot tystnadsplikt eller dataintrång. Även reglerna om disciplinansvar för tjänsteförseelse kan tillämpas i fråga om en anställd inom såväl det statliga som kommunala området.

Mot bakgrund av vad som nu sagts bedömer vi att det, vid sidan av skadeståndsansvaret enligt 48 § PuL, inte behöver införas några ytterligare sanktioner genom särskilda bestämmelser i den nya lagen som innebär att vissa överträdelser mot lagen också är straffsanktionerade. Vi lämnar därför inget förslag till några nya straffbestämmelser som ska gälla på myndighetsområdet.

Vår bedömning innebär också att det inte ska göras någon hänvisning till bestämmelsen om straff i 49 § PuL i den nya lagen.

18.2 Bemyndiganden

18.2.1 Bestämmelser som avviker från eller kompletterar den nya lagen

Den nya lagen innehåller bestämmelser som rör frågor där personuppgiftslagens bestämmelser inte på ett tillräckligt tydligt sätt uttrycker vad som gäller för myndigheters behandling av personuppgifter. Bestämmelserna reglerar alltså vad som ska gälla särskilt för myndigheterna i en viss fråga till skillnad från vad enskilda personuppgiftsansvariga har att iaktta. Den nya lagen förtydligar på detta sätt i materiellt hänseende vad som gäller för myndigheters behandling av personuppgifter i förhållande till personuppgiftslagen. Den kan därmed sägas ställa upp en mer fast ram för myndigheters behandling av personuppgifter. Det innebär i sin tur att behovet av sådana relativt vidsträckta bemyndiganden som ges i 50 § PuL minskar. Vi har emellertid i samband med våra överväganden i de olika avsnitten om enskilda sakfrågor redan konstaterat att den reglering som ges i lagen i vissa fall behöver kompletteras med mer detaljerade föreskrifter eller att det behöver ges utrymme för avvikande bestämmelser.

Vi har i avsnitt 7.3 redovisat vår uppfattning att vi från allmän normgivningssynpunkt inte ser några hinder mot att bestämmelser som avviker från innehållet i den generella lagen i form av t.ex. myndighetsspecifika föreskrifter om sökbegränsningar, direktåtkomst, behandling av känsliga personuppgifter m.m. ges i form av förordning. Såvitt avser statliga myndigheter under regeringen meddelas sådana föreskrifter med stöd av den s.k. restkompetensen (8 kap. 7 första stycket 2 RF).

I den mån bestämmelser som avviker från vad som föreskrivs i den generella lagen innebär åligganden för de kommunala myndigheterna krävs emellertid enligt 8 kap. 2 § första stycket 3 RF att lagen innehåller ett bemyndigande för regeringen att meddela föreskrifterna i förordning. Föreskrifter som innebär ökade befogenheter för kommuner kräver enligt samma lagrum också lagstöd. Om en kommun ges en befogenhet i lag krävs att en begränsning av den lagstadgade befogenheten också ges i lag eller med stöd av bemyndigande i lag. Det krävs därför ett bemyndigande i lag för regeringen att meddela sådana föreskrifter som innebär en begränsning av kommunala myndigheters befogenheter att behandla personuppgifter automatiserat enligt den generella lagen.

Även i fråga om sådana regleringar som är att se som ingrepp i enskilds personliga förhållanden krävs att lagen innehåller ett bemyndigande för regeringen att meddela föreskrifter (jfr 8 kap. 3 och 10 §§).

Om riksdagen enligt 8 kap. RF bemyndigar regeringen att meddela föreskrifter i visst ämne, kan riksdagen också medge att regeringen bemyndigar en förvaltningsmyndighet eller en kommun att meddela föreskrifter i samma ämne (8 kap. 10 §).

18.2.2 Våra överväganden och förslag

Förslag: I lagen ges regeringen eller den myndighet som regeringen bestämmer bemyndigande att meddela föreskrifter om när behandling av personuppgifter är tillåten, vilka krav som ställs på en personuppgiftsansvarig myndighet och att känsliga personuppgifter får behandlas, om det behövs med hänsyn till ett viktigt allmänt intresse. Regeringen bemyndigas också att meddela föreskrifter om begränsningar i möjligheterna att använda andra sökbegrepp än som avses i förslaget till 12 §.

Vi föreslår alltså en generell bestämmelse som tillåter en myndighet att behandla personuppgifter om det är nödvändigt för att myndigheten ska kunna utföra sina uppgifter. Det bör emellertid vara möjligt för regeringen att meddela föreskrifter om att det för en viss myndighet eller i en viss myndighetspecifik verksamhet ska gälla särskilda begränsningar i möjligheterna att behandla personupp-

gifter automatiserat. Om en sådan begränsning avser en kommunal myndighet innebär det en begränsning av vad som annars skulle ha gällt enlig lagen. Det behövs därför ett bemyndigande för regeringen att meddela denna typ av föreskrifter. Regeringen bör även medges att bemyndiga en myndighet att meddela föreskrifter i samma ämne. Bemyndigandet bör ges motsvarande utformning som 50 § a PuL.

Av samma skäl behövs ett bemyndigande för regeringen att meddela föreskrifter om ytterligare begränsningar i möjligheten att använda sökbegrepp utöver huvudregeln om sökförbud i fråga om känsliga personuppgifter i 13 §. I detta fall bör emellertid regeringen inte medges att vidaredelegera föreskriftsrätten, eftersom en sådan föreskrift inte skulle kunna utgöra en sådan sökbegränsning som avses i den s.k. begränsningsregeln i 2 kap. 3 § tredje stycket TF.

I lagen föreskrivs ett generellt undantag från förbudet i 13 § PuL mot att behandla känsliga personuppgifter som innebär att en myndighet tillåts att i viss uttryckligen begränsad omfattning behandla känsliga personuppgifter. I den mån sådan behandling kan anses utgöra ett ingrepp i enskilds personliga förhållanden finns således ett sådant lagstöd som krävs enligt 8 kap. 2 § första stycket 2 RF.

I likhet med vad som är fallet enligt 20 § PuL bör det emellertid finnas möjlighet för regeringen eller den myndighet som regeringen bestämmer att meddela ytterligare undantag från förbudet i 13 § samma lag om det behövs med hänsyn till ett viktigt allmän intresse. Ett sådant bemyndigande föreslås därför bli intaget i den generella lagen.

Vi föreslår vidare att det i den nya lagen tas in en bestämmelse som på ett tydligare sätt än 31 § PuL anger vad som krävs av myndigheter när det gäller deras skyldighet som personuppgiftsansvariga att vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder. Det kan emellertid förutsättas att det ändå kommer att finnas ett behov av mer specifika regler inom vissa sektorer eller för en viss myndighet eller verksamhet. Även en sådan bestämmelse kan innebära ett åliggande för en kommun och behöver därför hämta sitt stöd i ett bemyndigande i lagen. Ett sådant bemyndigande bör ges en sådan utformning att det också kan täcka in sådana fall då de grundläggande kraven i 9 § PuL i något avseende behöver preciseras, exempelvis om begränsande regler för direktåtkomst till personuppgifter som inte är sekretessreglerade behövs i fråga om en viss

myndighets verksamhet. Det bör därför ges ett motsvarande innehåll som 50 § b PuL.

Den nya lagen föreslås också innehålla en bestämmelse som föreskriver en generell skyldighet för myndigheter att föra en förteckning över de behandlingar av personuppgifter som myndigheten utför. Lagen bör emellertid inte tyngas av detaljerade föreskrifter om vilka uppgifter en sådan förteckning ska innehålla utan sådana föreskrifter bör meddelas av regeringen eller den myndighet som regeringen bestämmer. Dessa föreskrifter tillhör regeringens eget primärområde och något bemyndigande i lagen behövs därför inte. Däremot bör en upplysning om att regeringen eller en myndighet, efter vidaredelegation av regeringen, meddelar närmare föreskrifter i ämnet tas in i lagen i anslutning till huvudbestämmelsen.

18.3 Överklaganden

18.3.1 Allmänna dataskyddsrättsliga regler

Dataskyddsdirektivet

Enligt artikel 22 i dataskyddsdirektivet ska medlemsstaterna föreskriva att var och en har rätt att föra talan inför domstol om sådana kränkningar av rättigheter som skyddas av den nationella lagstiftningen som är tillämplig på behandling enligt direktivet.

I artikel 28.3, som innehåller bestämmelser om vilka undersökningsbefogenheter och befogenheter i övrigt som tillsynsmyndigheten ska ha för sin tillsyn, föreskrivs att sådana beslut av tillsynsmyndigheten som går en part emot kan överklagas till domstol.

Personuppgiftslagen

Rätten att överklaga tillsynsmyndighetens beslut

Direktivets krav på att tillsynsmyndighetens beslut som går en part emot ska kunna överklagas till domstol har genomförts i svensk lagstiftning genom 51 § PuL. Enligt den bestämmelsen får tillsynsmyndighetens beslut enligt personuppgiftslagen överklagas hos allmän förvaltningsdomstol. Det gäller emellertid inte tillsynsmyndighetens beslut om föreskrifter. Vidare ges tillsynsmyndigheten

befogenhet att besluta att dess beslut ska gälla även om det överklagas.

Högsta förvaltningsdomstolen har i rättsfallet RÅ 2010 ref. 29 funnit att Datainspektionens beslut, som genom en skrivelse meddelats den som framfört ett klagomål, att inte vidta någon åtgärd med anledning av ett klagomål inte är ett överklagbart beslut. Ett sådant beslut anses alltså inte ha gått part emot på det sätt som avses i 51 § PuL. Till stöd för den tolkningen har Högsta förvaltningsdomstolen anfört allmänna principer som har utbildats i praxis om vad som utgör ett överklagbart förvaltningsbeslut.

Rätten att överklaga vissa myndighetsbeslut

I 52 § PuL, som infördes år 2007, föreskrivs att en myndighets beslut om information enligt 26 §, om rättelse och underrättelse till tredje man enligt 28 §, om information enligt 29 § andra stycket och om upplysningar enligt 42 § får överklagas hos allmän förvaltningsdomstol. Rätten att överklaga gäller dock inte beslut av riksdagen, regeringen eller riksdagens ombudsmän.

Direktivets krav enligt artikel 22 att medlemsstaterna ska föreskriva en rätt för var och en att föra talan om kränkningar av rättigheter enligt den nationella lagstiftningen medförde inte några särskilda lagstiftningsåtgärder vid personuppgiftslagens införande. Frågan behandlades inte heller närmare i förarbetena utom beträffande rätten att begära att en personuppgift korrigeras enligt 28 §. Regeringen anförde rörande en sådan begäran att om oenighet uppstod mellan den personuppgiftsansvarige och den registrerade om huruvida korrigering skulle ske, kunde den registrerade vända sig till tillsynsmyndigheten (prop. 1997/98:44 s. 86). Regeringen erinrade också om möjligheten att själv väcka talan vid allmän domstol. Det får således antas att den bedömningen gjordes att vars och ens rätt att väcka talan vid allmän domstol i den ordning som gäller för tvistemål ansågs vara tillräcklig för att uppfylla direktivets krav i denna del.

Den särskilda bestämmelsen om överklagande i 52 § PuL infördes som en följd av den översyn av personuppgiftslagen som Personuppgiftslagsutredningen gjorde (SOU 2004:6). Bakgrunden var enligt förarbetena i huvudsak följande (prop. 2005/06:173 s. 51 f.). Rege-

ringen konstaterade inledningsvis att tillämpningen av allmänna förvaltningsrättsliga principer torde leda till att åtminstone vissa myndighetsbeslut enligt personuppgiftslagen kunde överklagas, trots avsaknad av uttryckliga bestämmelser om det i lagen. I samband med utformningen av särskilda registerlagar efter införandet av personuppgiftslagen hade det ofta bedömts att myndighetsbeslut som direkt berör den enskilde skulle kunna överklagas. Myndighetsbeslut som ansetts vara interna eller administrativa – t.ex. att inrätta ett register – och således inte direkt berör den enskilde bedömdes däremot inte vara av sådant slag att de borde kunna överklagas. Det hade därför ofta införts bestämmelser i registerförfattningar som gav den registrerade rätt att till allmän förvaltningsdomstol överklaga beslut om rättelse och om information som ska lämnas enligt 26 § PuL (s.k. registerutdrag). Det påpekades att bilden dock var något splittrad i fråga om existensen och utformningen av bestämmelser om överklagande i särskilda registerlagar. Den rättsliga fråga som en överklaganderätt i den särskilda registerlagen tog sikte på reglerades däremot ofta i sin helhet i personuppgiftslagen. Lagrådet hade i några lagstiftningsärenden framfört synpunkten att bestämmelser om överklagande i sådana fall av systematiska skäl borde införas i personuppgiftslagen och inte i den särskilda registerlagen (se t.ex. prop. 2002/03:40 s. 241). Enligt regeringen var det inte tillfredsställande att bestämmelser om överklagande av beslut fanns i en lag och bestämmelser om beslutens meddelande i en annan. Till detta kom att inte alla myndigheters personuppgiftsbehandling reglerades i en särskild registerförfattning. Dessa myndigheter stödjer i stället sin behandling direkt på personuppgiftslagen. För att avgöra om sådana myndigheters beslut enligt lagen kan överklagas måste utgångspunkt tas i allmänna förvaltningsrättsliga principer om överklagande i stället för en uttrycklig bestämmelse i lagen. Mot bakgrund av dessa förhållanden borde det, som utredningen föreslagit, i personuppgiftslagen införas särskilda bestämmelser om överklagande av myndighetsbeslut.

Förslaget till uppgiftsskyddsförordning

I kommissionens förslag till uppgiftsskyddsförordning föreskrivs i artikel 74.1 att varje fysisk eller juridisk person ska ha rätt till ett rättsmedel mot beslut som en tillsynsmyndighet har fattat med avseende på vederbörande.

Av artikel 74.3 följer att en sådan talan ska ges in vid domstolarna i den medlemsstat där tillsynsmyndigheten har sitt säte.

I artikel 75.1 föreskrivs att varje fysisk person som anser att hans eller hennes rättigheter enligt denna förordning har åsidosatts som en följd av att personuppgifter har behandlats på ett sätt som inte är förenligt med förordningen ska ha rätt att begära domstolsprövning.

Enligt artikel 75.2 ska en sådan talan väckas vid domstolarna i den medlemsstat där den registeransvarige eller registerföraren är etablerad. Alternativt får sådan talan väckas vid domstolarna i den medlemsstat där den registrerade har hemvist, såvida inte registerföraren är en offentlig myndighet som agerar inom ramen för sin myndighetsutövning.

Några kommentarer

Det kan konstateras att bestämmelserna i förslaget till förordning om överklaganden av tillsynsmyndighetens beslut och möjligheterna att föra talan om kränkningar bygger på dataskyddsdirektivets bestämmelser. I förordningen finns emellertid också förslag till forumregler. Om förordningen införs, behövs ju forumregler eftersom förordningen blir direkt tillämplig i varje medlemsstat. På myndighetsområdet innebär förslagen till forumregler emellertid i princip inga skillnader jämfört med vad som redan gäller enligt svenska regler.

18.3.2 Allmänna bestämmelser om överklagande av myndighetsbeslut

Enligt 22 § FL, får ett beslut överklagas av den som beslutet angår, om det har gått honom emot och beslutet kan överklagas.

I bestämmelsen finns således en allmän regel om vem som har rätt att överklaga en myndighets beslut. Frågan om klagorätt hänger nära samband med frågan om beslutet över huvud taget är överklagbart. Regler om det finns i specialförfattningar och myndighetsinstruktioner. Det finns också överklagbarhetsregler som gäller på sedvanerättslig grund (se Hellners/Malmqvist, kommentaren till 22 §).

I 22 a § föreskrivs att beslut som huvudregel överklagas hos allmän förvaltningsdomstol. I sådana fall krävs prövningstillstånd vid överklagande till kammarrätten. Beslut i anställningsärenden eller i normgivningsärenden undantas emellertid från bestämmelsens tillämpningsområde.

Paragrafen infördes år 2006. Syftet var bl.a. att förebygga negativa kompetenskonflikter mellan de allmänna domstolarna och de allmänna förvaltningsdomstolarna (Hellners/Malmqvist, kommentaren till 22 a §). Bestämmelsen innebär att frågan om ett myndighetsbeslut är överklagbart numera prövas av förvaltningsdomstol, utom såvitt avser anställnings- eller normgivningsärenden. Den tidigare oskrivna regeln om att man i sista hand kunde överklaga till regeringen har därmed övergetts.

18.3.3 Våra överväganden och förslag

Möjligheten att överklaga tillsynsmyndighetens beslut

Förslag: Tillsynsmyndighetens beslut enligt lagen om annat än föreskrifter ska kunna överklagas till allmän förvaltningsdomstol. Ett sådant beslut ska kunna gälla även om det överklagas, om tillsynsmyndigheten beslutar om detta.

Allmänt om förutsättningarna för en myndighet att överklaga en annan myndighets beslut

De förvaltningsrättsliga principerna om klagorätt anses ha tillämpning också på myndigheter när de uppträder i någon privaträttslig egenskap, exempelvis som arbetsgivare eller fastighetsägare (Hellners /Malmqvist, kommentaren till 22 §). I en sådan egenskap har en myndighet alltså samma rätt att överklaga som enskilda. När myndigheter däremot uppträder i sin offentligrättsliga skepnad är förhållandena annorlunda. Härvidlag är det grundläggande synsättet annorlunda beträffande myndigheter i kommuner och landsting än för statliga myndigheter. Som huvudregel gäller att en statlig myndighet endast har rätt att överklaga en annan myndighets beslut när detta är särskilt föreskrivet. I andra fall saknas alltså klagorätt. På det kommunala området kan däremot en rätt att överklaga finnas även utan särskilt författningsstöd, om beslutet berör sådana allmänna, till kommunen knutna intressen som exempelvis trafik, ordning och trivsel och att det i speciallagstiftningen på området i fråga har tagits hänsyn till de kommunala intressena.

Om det saknas ett särskilt författningsstöd för en statlig myndighet som lyder under regeringen att överklaga en annan sådan statlig myndighets beslut anses allmänt gälla att en tvistig fråga ytterst kan avgöras av regeringen. Det är därför 6 kap. 8 § fjärde stycket OSL föreskriver att ett beslut av en statlig myndighet som lyder under regeringen att vägra att lämna ut en uppgift till en annan sådan statlig myndighet enligt 6 kap. 5 § OSL överklagas till regeringen. I förarbetena till bestämmelsen anfördes att det ibland kan innebära att en svår och känslig avvägning måste ske när det gäller att lösa tvister mellan statliga myndigheter i frågor som det här gäller. Vid denna avvägning träder mera sällan de rent rättsliga aspekterna i förgrunden (prop. 1979/80:2 Del A s. 364).

Rätten att överklaga enligt dataskyddsdirektivet

Det är ett krav enligt dataskyddsdirektivet att tillsynsmyndighetens beslut när den utövar sina tillsynsbefogenheter ska kunna överklagas till domstol. Om förslaget till uppgiftsskyddsförordning blir verklighet kommer en sådan rätt att följa direkt av förordningen. Något undantag görs alltså inte för myndigheters rätt att överklaga.

Även om man kan tycka att det är en något udda företeelse att det förekommer processer i allmän förvaltningsdomstol mellan tillsynsmyndigheten – som är en statlig myndighet som lyder under regeringen – och andra statliga myndigheter som också lyder under regeringen, kräver direktivet alltså att även myndigheter såsom personuppgiftsansvariga ska ha en möjlighet att kunna överklaga tillsynsmyndighetens beslut. Vi tycker oss kunna skönja en tendens att processer av det här slaget har blivit vanligare. Detta torde i viss mån hänga samman med tillsynsmyndighetens val av metod för åtgärder riktade mot myndigheters behandling av personuppgifter. I den mån tillsynsmyndigheten beslutar om föreskrifter snarare än att agera genom tillsynsbeslut mot enskilda myndigheter minskar antalet överklagbara beslut.

Det skulle naturligtvis kunna diskuteras, av samma skäl som anfördes beträffande den särskilda instansordningen som gäller då myndigheter tvistar om skyldigheten att utbyta uppgifter, om det inte vore lämpligare att regeringen löste tvister mellan tillsynsmyndigheten och andra statliga myndigheter under regeringen när det gäller vilka krav som bör ställas på behandlingen av personuppgifter, exempelvis i fråga om vilken skyddsnivå som olika säkerhetsåtgärder bör ligga på. Som redan påpekats följer emellertid av såväl dataskyddsdirektivet som förslaget till uppgiftsskyddsförordning ett krav på att samtliga personuppgiftsansvariga ska ha rätt att överklaga tillsynsmyndighetens beslut till domstol. Det kan vidare knappast komma i fråga att föreskriva att en kommunal myndighets överklagande av tillsynsmyndighetens beslut ska ske till regeringen. Samtliga myndigheters överklaganden av tillsynsmyndighetens beslut bör därför, liksom hittills, ske till allmän förvaltningsdomstol.

Eftersom vi föreslår att tillsynsmyndighetens samtliga befogenheter gentemot myndigheterna bör regleras i den nya lagen, bör den lagen även en innehålla en bestämmelse som föreskriver en rätt att överklaga tillsynsmyndighetens beslut. I sak anser vi att den bör vara i princip likalydande med 51 § PuL.

Möjligheten att överklaga en myndighets beslut i egenskap av personuppgiftsansvarig

Förslag: En myndighets beslut enligt den nya lagen om rättelse eller komplettering, om avskiljande eller utplåning och om rätt till information ska kunna överklagas till allmän förvaltningsdomstol. Någon rätt att överklaga sådana beslut av regeringen, Högsta domstolen, Högsta förvaltningsdomstolen eller riksdagens ombudsmän ska emellertid inte finnas.

Några andra beslut som en myndighet fattar enligt den nya lagen ska inte kunna överklagas.

En överklagandebestämmelse bör införas i den nya lagen

Personuppgiftslagen innehöll alltså ursprungligen inte några bestämmelser om överklaganden av beslut som en myndighet fattar i egenskap av personuppgiftsansvarig. Skälet till detta kan ha varit att den rätt att föra talan som föreskrivs i artikel 22 i dataskyddsdirektivet uppfattades avse enbart ett sådant civilrättsligt förhållande där tvister ska lösas i allmän domstol. Även en personuppgiftsansvarig myndighet torde alltså i detta sammanhang ha uppfattas som ett privaträttsligt subjekt som tvistar mot ett annat sådant. Om en personuppgiftsansvarig som är ett enskilt rättssubjekt beslutar sig för att exempelvis inte tillmötesgå en begäran från en registrerad att upphöra med behandling av känsliga personuppgifter som rör denne, måste det givetvis finnas en möjlighet att få tvisten löst i allmän domstol. Den personuppgiftsansvarige kan ju i en sådan situation inte ensidigt få råda över vad som ska gälla.

Några uttryckliga bestämmelser som reglerar vad som gäller i fråga om överklagbarhet när en myndighet uppträder som part i ett civilrättsligt förhållande och i den egenskapen fattar beslut, exempelvis s.k. partsbesked, finns inte. Normalt saknas möjlighet för motparten då tvist uppstår i ett sådant förhållande att få tvisten löst av allmän förvaltningsdomstol genom överklagande av myndighetens beslut. Ett överklagande av ett sådant beslut kommer att avvisas av domstolen. Beslut av det slag som är aktuella nu faller nämligen utanför begreppet myndighetsutövning, eftersom saken i dessa fall inte avgörs ensidigt av myndigheten (Hellners/Malmqvist, kom-

mentaren till 22 §). I den mån överklagbarhet saknas, får alltså en tvist lösas i civilrättslig ordning i allmän domstol.

När överklagandebestämmelsen infördes i 52 § PuL förefaller det emellertid ha setts som en självklarhet att beslut som myndigheten fattar i egenskap av personuppgiftsansvarig i princip utgör ett utflöde av dess myndighetsutövning och inte någon form av ställningstagande i ett civilrättsligt förhållande. Det synsättet hade tidigare anlagts i olika lagstiftningsärenden rörande registerförfattningar. Frågan i dessa lagstiftningsärenden var snarare i vilken mån myndighetens tillämpning av lagens olika bestämmelser ur ett förvaltningsrättsligt perspektiv utgjorde ett överklagbart beslut. Normalt anlades det synsättet att beslut som direkt berör den enskilde skulle kunna överklagas på samma sätt som andra förvaltningsbeslut, dvs. till allmän förvaltningsdomstol (se t.ex. prop. 2000/01:33 s. 109). Ett beslut av det slaget ansågs det bl.a. vara fråga om då en myndighet tillämpar 28 § PuL om rättelse. Överklaganderätten skulle däremot inte omfatta beslut som avsåg interna eller administrativa frågor, exempelvis i samband med att ett register inrättas.

Det kan konstateras att det får anses naturligt att se en myndighets beslut i egenskap av personuppgiftsansvarig, exempelvis i fråga om en personuppgift ska rättas eller inte, som ett utflöde av dess myndighetsutövning. I allmänhet har ju myndigheten samlat in sina personuppgifter i syfte att kunna utföra förvaltningsuppgifter. Uppgifterna har också många gånger samlats in med stöd av olika författningsbestämmelser oberoende av om de registrerade har getts möjlighet att samtycka till insamlingen eller inte. Detta skiljer i betydande mån den behandling av personuppgifter som sker hos myndigheter från den behandling som sker hos personuppgiftsansvariga som utgör enskilda rättssubjekt. I det senare fallet har t.ex. personuppgifter som huvudregel ursprungligen samlats in med stöd av samtycke från den registrerade.

Vi anser därför att den generella lagen bör innehålla en bestämmelse som föreskriver att vissa beslut som fattas när en myndighet tillämpar lagens bestämmelser ska kunna överklagas till allmän förvaltningsdomstol. Nedan behandlar vi vilka beslut som bör omfattas.

Vilka beslut enligt lagen ska kunna överklagas?

När det gäller den registrerades rätt att överklaga en myndighets beslut enligt den nya lagen som myndigheten fattar i egenskap av personuppgiftsansvarig bör enligt vår uppfattning samma utgångspunkt gälla som i fråga om rätten att överklaga beslut enligt personuppgiftslagen. Överklaganderätten bör alltså enbart ta sikte på sådana beslut av myndigheten som direkt berör den enskilde. Sådana beslut bör alltså kunna överklagas på samma sätt som andra förvaltningsbeslut.

Vi anser alltså att den registrerade ska kunna överklaga beslut då en myndighet med stöd av den nya lagen beslutar om rättelse eller komplettering, om avskiljande eller utplåning och om rätt till information. Besluten ska överklagas till allmän förvaltningsdomstol. Rätten att överklaga ska emellertid inte omfatta beslut av regeringen, Högsta domstolen, Högsta förvaltningsdomstolen eller JO.

Bestämmelsen om rätt att överklaga en myndighets beslut enligt 22 § FL och forumbestämmelsen för ett sådant överklagande i 22 a § samma lag gäller generellt.

Av 3 § FL följer emellertid att om en annan lag eller förordning innehåller någon bestämmelse som avviker från denna lag, gäller den bestämmelsen.

Det är enbart sådana beslut som räknas upp i bestämmelsen om överklagande i den nya lagen som ska kunna överklagas. För att det ska bli tydligt att någon rätt att överklaga andra beslut som en myndighet fattar med stöd av lagen än de som räknas upp i bestämmelsen inte heller ska finnas enligt förvaltningslagen, bör det uttryckligen framgå av en bestämmelse i den nya lagen att ett förbud mot att överklaga sådana beslut gäller.

19 Konsekvenser

19.1 Det framtida lagstiftningsarbetet med utgångspunkt i en ny lag om myndigheters behandling av personuppgifter

19.1.1 Allmänna konsekvenser

En gemensam rättslig ram

Den nya lagen innehåller en i princip generell reglering av myndigheters behandling av personuppgifter. Därigenom ges regler som kan utgöra en ändamålsenlig reglering för flertalet av de frågor som är centrala för den personuppgiftsbehandling som sker i både statliga och kommunala myndigheters verksamhet. Genom den nya lagen ges myndigheterna således en gemensam rättslig ram för behandlingen av personuppgifter på samma sätt som exempelvis förvaltningslagen utgör en gemensam grund för de krav som ställs på myndigheterna i förvaltningsrättslig bemärkelse.

Behovet av särreglering minskar avsevärt

Framväxten av särskilda registerförfattningar har bl.a. haft sin grund i synsättet att det är ändamålsenligt att viss sektorsvis personuppgiftsbehandling får sin egen reglering. Konsekvensen har emellertid blivit att registerförfattningarna, i synnerhet kategorin informationshanteringsförfattningar, i hög grad kommit att innehålla likartade bestämmelser som rör frågor av generellt slag exempelvis om personuppgiftsansvarets placering, när personuppgifter kan behandlas och tillåtelse att behandla känsliga personuppgifter. De innehåller också likartade lösningar för hur personuppgiftslagens bestämmelser om en registrerads rätt till information, om rättelse

och korrigering, tillsynsmyndighetens befogenheter samt sanktioner vid en otillåten behandling ska bli tillämpliga även i fråga om regleringen i registerförfattningarna. Behovet av att reglera dessa frågor särskilt har i allmänhet inte haft sin grund i speciella omständigheter som rör just den aktuella myndigheten eller verksamheten, utan har ofta motiverats utifrån principiella och generella resonemang som snarare rör myndighetsverksamhet rent allmänt. Genom den nya lagen får dessa frågor en reglering som i betydligt högre grad än vad som är fallet med personuppgiftslagen har utformats mot bakgrund av både principiella och sakliga resonemang där utgångspunkten är myndigheters verksamhet och den rättsliga miljö som sådan verksamhet befinner sig i. Regleringen i den nya lagen är därför avsevärt mer ändamålsenlig än personuppgiftslagen när det gäller myndigheters behov av att kunna behandla personuppgifter i sin verksamhet. Därmed innebär den nya lagen att det i det framtida lagstiftningsarbetet inte kommer att finnas samma behov av att i en från lagen avvikande eller kompletterande reglering särskilt reglera frågor av generell karaktär som rör myndigheters behandling av personuppgifter. Eftersom många registerförfattningar till stor del innehåller denna typ av bestämmelser innebär det att framtida särreglering kan ges en avsevärt mer begränsad omfattning.

Den nya lagen medför att behovet av särreglering i princip enbart kommer att ta sikte på sådant som har sin grund i speciella omständigheter som rör just den aktuella myndigheten eller sektorsvisa verksamheten. Enligt vår uppfattning kommer behovet därför i princip att vara begränsat till frågor som rör författningsstöd för direktåtkomst, sökbegränsningar, gallring för att skydda personuppgifter och, i rena undantagsfall, ytterligare möjligheter att behandla känsliga personuppgifter. Det kan inte heller uteslutas att det även framöver kommer att på något visst område eller för viss informationssamling anses behövas snävare förutsättningar än vad som följer av de generella bestämmelserna i den nya lagen. Sådana frågor kan t.ex. avse vilka personuppgiftskategorier som får eller inte får behandlas eller särskilda krav på tekniska eller organisatoriska säkerhetsåtgärder som ska gälla på visst område.

Den nya lagen är tänkt att kunna kompletteras med en eller flera bilagor. I bilagor till lagen respektive i en till lagen anslutande förordning kan särreglering rörande t.ex. direktåtkomst, sökbegränsningar,

gallring för att skydda personuppgifter och tillåtelse att behandla känsliga personuppgifter m.fl. frågor tas in beroende på vilken normnivå regleringen bör eller behöver ges. Behovet av att vid sidan av den nya lagen och den anslutande förordningen införa särskilda registerförfattningar kommer därmed att begränsas till de fall då sådana författningar behöver innehålla andra bestämmelser som inte har anknytning till persondataskydd, exempelvis om uppgiftsskyldighet, registreringsförfarande eller om information eller annan service. Ett behov av en särskild författning kan också finnas när behovet av särregler är så omfattande att det inte är lämpligt att föra in dem i en bilaga till lagen eller i den anslutande förordningen.

Revidering av nu gällande registerförfattningar

Den nya lagen är utformad så att den är subsidiär i förhållande till avvikande bestämmelser i annan lag eller förordning. Det innebär att den reglering som i dag finns i registerförfattningar inte påverkas av att den nya lagen införs i så måtto att dessa författningar ändras eller upphävs och inte heller att en revidering behöver ske efter en viss tid. Det står alltså lagstiftaren fritt att helt avstå från att revidera gällande registerförfattningar för att anpassa dem efter den nya lagens bestämmelser och de utgångspunkter som den bygger på. I den mån lagstiftaren däremot vill anpassa gällande regler till den nya lagen, kan det ske i den utsträckning och form samt vid den tidpunkt som det befinns lämpligt.

Även om behovet av den nya lagen främst har sin grund i de problem som vi anser är förknippade med kategorin informationshanteringsförfattningar, finns det inget som hindrar att lagstiftaren låter lagens utgångspunkter beträffande exempelvis elektroniskt uppgiftsutlämnande få genomslag också i fråga om s.k. renodlade registerförfattningar. Detsamma kan även gälla frågeställningar som t.ex. tillsynsmyndighetens befogenheter. Inget hindrar t.ex. att dataskyddsreglering i en renodlad registerförfattning, som efter en översyn fortfarande anses behövas, separeras från registerförfattningen och förs över till bilaga till den nya lagen eller anslutande förordning. Registerförfattningen blir därefter en mer renodlad verksamhetsreglering exempelvis rörande anmälnings- och registreringsförfarande m.m. Vi för vår del ser under alla förhållanden bety-

dande fördelar med att sådana för alla myndigheter gemensamma frågor får en reglering som på så stora områden som möjligt bygger på samma utgångspunkter. Det leder till förbättrad överblick och ökade möjligheter till samordning.

19.1.2 Vissa särskilda konsekvenser

Avreglering beträffande ändamålsbestämmelser

Den nya lagen innehåller en generell rättslig grund för när myndigheters behandling av personuppgifter över huvud taget kan vara tillåten. Den rättsliga grunden, som avses ersätta 10 § PuL, är knuten till att behandlingen ska vara nödvändig för myndigheters verksamhet, dvs. för verksamhet som förutsätts bedrivas. Lagen innehåller inga bestämmelser om för vilka ändamål som myndigheter får behandla personuppgifter. Enligt vårt förslag ska alltså huvudregeln vara att det är myndigheten själv som, inom ramarna för sina uppgifter och befogenheter, har att närmare specificera för vilka särskilda, uttryckliga och berättigade ändamål personuppgifter behandlas i verksamheten (9 § första stycket c PuL).

Bakgrunden till huvudregeln är att vi från såväl systematiska som integritetsmässiga synpunkter ser nuvarande ändamålsbestämmelser i registerförfattningar som problematiska. Detta har vi närmare utvecklat i avsnitt 9.2.4. Som har framgått där är det vår bedömning att ändamålsbestämmelser i registerförfattningar ofta snarare utgör preciseringar av de rättsliga grunderna för personuppgiftsbehandling i den reglerade verksamheten än ändamålsbestämningar som lever upp till dataskyddsregleringens krav på att vara särskilda, dvs. inte för vida eller vaga. Vi har också sett lagstiftarens sammanblandning mellan rättsliga grunder och ändamålsbestämning som riskfylld från integritetssynpunkt då det kan leda till passivitet från den reglerade myndighetens sida när det gäller att själv för olika delar av sin totala informationshantering avgränsa personuppgiftsbehandlingarna med ändamålsbestämningar som lever upp till de grundläggande kraven på att vara tillräckligt specifika.

Enligt vår mening bör man i det framtida lagstiftningsarbetet ha som utgångspunkt att ändamålsbestämmelser ska införas bara då det finns ett verkligt behov av sådana bestämmelser för att i reell mening begränsa en myndighets ”behandlingsutrymme” i förhållande till vad

som följer av de generella reglerna. Så kan exempelvis vara fallet i fråga om användningen av vissa särskilt känsliga uppgiftssamlingar, t.ex. för att snäva in för vilka syften en annan myndighet får använda sin direktåtkomst till uppgiftssamlingen. Vidare kan det – i det fortsatta arbetet med revidering av befintliga registerförfattningar – finnas anledning att se över befintliga ändamålsbestämmelser med samma utgångspunkt, dvs. att ändamålsbestämmelser bara bör finnas i de fall det finns ett verkligt behov av sådana bestämmelser.

Avreglering beträffande elektroniskt utlämnande

Direktåtkomst

Genom den nya lagen klargörs att direktåtkomst till sekretessreglerade personuppgifter som huvudregel ska ha stöd i lag eller förordning. Bortsett från sådana registerförfattningar som innehåller ett förbud mot direktåtkomst utan stöd i lag eller förordning regleras inte frågan i någon annan lagstiftning. När lagen träder i kraft kommer detta krav därför att gälla för alla myndigheter oavsett vilken reglering som styr deras personuppgiftsbehandling.

I offentlighet- och sekretesslagen införs en ny bestämmelse som innebär att en bestämmelse i lag eller förordning som ger stöd för direktåtkomst till sekretessreglerade uppgifter är sekretessbrytande i sig. Den bestämmelsen innebär att den hittills tillämpade ordningen med särskilda sekretessbrytande regler vid sidan av bestämmelser om direktåtkomst inte länge behövs. Direktåtkomst till sekretessreglerade uppgifter kan därför i det framtida lagstiftningsarbetet möjliggöras genom en och samma bestämmelse.

I fråga om direktåtkomst till personuppgifter som inte är sekretessreglerade saknar lagen bestämmelser. Skälet till det är att någon motsvarande reglering som beträffande sekretessreglerade uppgifter enligt vår uppfattning inte i tillräckligt hög grad kan motiveras utifrån ett integritetsskyddsperspektiv. Däremot har vi lämnat förslag om krav på föregående risk- och sårbarhetsanalys och överenskommelser med mottagare i säkerhetsfrågor m.m. Generellt sett ser vi alltså inget som hindrar att en myndighet själv får avgöra om direktåtkomst till personuppgifter som inte är sekretessreglerade ska medges. Det kan dock förekomma att en reglering som begränsar en myndighets möjlighet att medge direktåtkomst till sådana person-

uppgifter kan behövas inom en viss sektor. Vårt val att i den nya lagen inte införa regler som generellt begränsar myndigheternas möjlighet att göra egna bedömningar i denna fråga syftar emellertid till att man i det framtida lagstiftningsarbetet bör ha som utgångspunkt att sådana begränsningar endast bör införas för de myndigheter eller sektorer där det finns ett verkligt behov.

Om direktåtkomst har medgetts i en nu befintlig registerförfattning finns det normalt sett dels en bestämmelse som medger direktåtkomst, dels en sekretessbrytande regel som ska möjliggöra det utlämnande som sker genom direktåtkomsten. En anpassning till den nya bestämmelsen i offentlighets- och sekretesslagen kan ske på så sätt att bestämmelsen om direktåtkomst ses över så att den får åsyftad sekretessbrytande effekt, vilket sker genom att bestämmelsen ges tillräcklig konkretion i fråga om vad direktåtkomsten ska avse, varefter den särskilda sekretessbrytande regeln kan upphävas.

Annat elektroniskt utlämnande

Den nya lagen saknar – förutom rörande direktåtkomst – regler om elektroniskt utlämnande till andra myndigheter. Skälet till det är att myndigheter enligt vår uppfattning ska kunna utgå från att en annan myndighet som man samverkar med följer de regler och uppfyller de krav som gäller för den verksamheten. Om personuppgifter får lämnas ut till en annan myndighet saknas det därför skäl att från integritetsskyddssynpunkt begränsa i vilken utsträckning eller på vilket sätt det kan ske i elektronisk form. Det bör alltså stå myndigheter fritt att – bortsett från när det gäller direktåtkomst till sekretessreglerade personuppgifter – utifrån övriga regelverk avgöra på vilket sätt personuppgifter lämpligen bör utbytas mellan dem.

Såvitt avser utlämnande till enskilda innehåller den nya lagen en bestämmelse som erinrar om att personuppgifter kan lämnas ut i elektronisk form, om de får lämnas ut och det inte är olämpligt att det sker på detta sätt. Syftet med denna bestämmelse är dels att erinra om att frågan om personuppgifter får lämnas ut ska bedömas skild från frågan om på vilket sätt uppgifterna ska lämnas ut. När det gäller den sistnämnda frågan är syftet med bestämmelsen att understryka att utgångspunkten bör vara att personuppgifter som

får lämnas ut, kan lämnas ut i elektronisk form. Endast om detta i det enskilda fallet är olämpligt bör ett annat sätt för utlämnande väljas.

I befintliga registerförfattningar är det vanligt med bestämmelser som begränsar en myndighets möjlighet att lämna ut personuppgifter i elektronisk form, i synnerhet såvitt avser utlämnande till enskilda. Som vi ser det bör bestämmelser i sådana författningar som begränsar elektroniskt utlämnande till andra myndigheter i princip genomgående kunna upphävas. När det gäller utlämnande till enskilda bör begränsande bestämmelser endast behållas om det finns ett verkligt behov av detta för att personuppgifter i tillräckligt hög rad ska skyddas i den aktuella myndighetens verksamhet.

Större möjlighet till överblick och samordning

Den nya lagen ska ses mot den bakgrunden att användningen av it i dag genomsyrar myndigheternas hela verksamhet och således numera utgör basen för framställning av dokument, ärendehantering, lagring, kommunikation och samverkan. Den elektroniska informationshanteringen utgör alltså inte längre någon särskild del av myndigheternas förvaltning, utan utgör i själva verket förvaltningen. Frågor som rör behandling av personuppgifter och hur ett tillräckligt skydd för uppgifterna kan uppnås inom ramen för en myndighets verksamhet kan således inte hanteras separat utan måste relateras till vad som gäller för verksamheten i övrigt och vilka krav som ställs där samt vilka samlade resurser som därmed behöver ställas till myndighetens förfogande. Dessa frågor är därför i hög grad en del av de förvaltningspolitiska frågorna i generell mening. Inte heller frågor som rör vilka krav på säkerhet som bör gälla vid behandling av personuppgifter kan avgöras separerat från de krav som i övrigt gäller för informationssäkerhet hos myndigheter. Genom den nya lagen ges emellertid en förbättrad möjlighet till överblick och samordning av hur både frågor om behandling av personuppgifter bör hanteras inom ramen för det allmänna förvaltningsuppdraget och i förhållande till myndighetsgemensamma krav på informationssäkerhet.

En orsak till att registerförfattningarna i hög grad uppvisar en splittrad bild i fråga om vad som gäller för myndigheters person-

uppgiftsbehandling kan vara att det i Regeringskansliet saknas tillräckliga möjligheter till samordning och överblick för dessa lagstiftningsfrågor. Det kommer givetvis även framöver att vara så att det är behörigt fackdepartement som har bäst inblick i frågor som rör vilka behov som kan finnas av särreglering i vissa frågor för en särskild myndighet eller verksamhet som hör till departementet i fråga. Om den nya lagen införs kommer emellertid överblicken och samordningen av de centrala frågor som rör myndigheters behandling av personuppgifter att hanteras av en och samma enhet inom Regeringskansliet, rimligen den som har ansvarat för lagstiftningsarbetet rörande den nya lagen. Detta kommer som vi ser det – förutom att lagen i sig leder till enhetlighet i fråga om begreppsanvändning – att leda till förbättrade möjligheter för lagstiftaren att upprätthålla en enhetlig syn på vad som bör gälla beträffande myndigheters behandling av personuppgifter.

19.2 Den nya lagen och ett införande av en unionsrättslig uppgiftsskyddsförordning

19.2.1 Allmänna iakttagelser

Innehållet i en blivande EU-förordning om behandling av personuppgifter – en uppgiftsskyddsförordning – är i skrivande stund inte fastlagt. Vad som kan förväntas bli innehållet i en sådan förordning kan inte heller fullt ut överblickas, i synnerhet inte på myndighetsområdet.

När uppgiftsskyddsförordningen träder i kraft kommer den att gälla direkt i samtliga medlemsstater och förutsätter således inte att dess innehåll genomförs i nationell lagstiftning. I princip kan nationell lagstiftning som rör behandling av personuppgifter alltså enbart införas i den utsträckning förordningen lämnar utrymme för att den kompletteras på detta sätt.

När det gäller myndigheters behandling av personuppgifter kan det emellertid förväntas att förordningen i viss utsträckning kommer att lämna särskilt utrymme för medlemsstaterna att ha en särreglering där frågor då kan ges lösningar som utformas efter nationella regelverk och andra speciella förutsättningar för de egna myndigheternas verksamhet. Förslaget till förordning är vidare i vissa frågor uppbyggt så att förordningen innehåller huvudregler med möjligheter

till undantag som tar hänsyn till vissa behov, bl.a. den behandling som kan behöva ske med hänsyn till ett allmänt intresse. Även på så sätt kan förordningen förväntas ge utrymme för nationell särlagstiftning där de egna myndigheternas behov kan beaktas.

Det kan också konstateras att en del av de bestämmelser som den nya lagen innehåller inte rör frågor som regleras vare sig i dataskyddsdirektivet eller förslaget till uppgiftsskyddsförordning. Det rör exempelvis frågorna om direktåtkomst och annat elektroniskt utlämnande samt sökbegränsningar.

19.2.2 Särskilda iakttagelser

I det följande redovisar vi hur vi ser på i vilken utsträckning bestämmelserna i den nya lagen kan fortsätta att gälla om uppgiftsskyddsförordningen införs. Dessa frågor har också delvis behandlats tidigare i de olika avsnitten rörande de enskilda sakfrågorna där vi i förekommande fall kommenterar hur dataskyddsdirektivets respektive förordningens bestämmelser förhåller sig till varandra. För en mer detaljerad beskrivning av de olika frågorna hänvisar vi därför till de kommentarerna.

Det ska observeras att bedömningarna i det följande i första hand förhåller sig till uppgiftsskyddsförordningen i dess ursprungliga version i kommissionens förslag från den 25 januari 2012.

Bestämmelser som kan komplettera en förordning

Den nya lagens bestämmelser om tillämpningsområde och syfte är enligt vår bedömning en självständig reglering som inte nödvändigtvis måste ändras även om lagen som sådan delvis måste omformas till en lag med till uppgiftsskyddsförordningen anslutande kompletterande reglering. Vi bedömer också att bestämmelsen om att lagen är subsidiär till annan nationell reglering i lag eller förordning kan behållas.

Bestämmelsen om att myndigheten ska vara personuppgiftsansvarig för den behandling som myndigheter utför och klargörandet av vad det innebär vid direktåtkomst bedömer vi vara en tillåten komplettering till förordningen.

Bestämmelserna i den nya lagen som rör särskilda kategorier av personuppgifter, dvs. beträffande känsliga personuppgifter samt personnummer och samordningsnummer, bedöms kunna gälla även som en komplettering till förordningen. Detsamma gäller bestämmelsen om sökförbud och samtliga bestämmelser om elektroniskt utlämnande, eftersom de frågorna över huvud taget inte regleras inom ramen för förordningen.

Undantagen i den nya lagen från förbudet mot överföring till tredjeland bedöms också vara en tillåten komplettering då de kommer att baseras på en särskild möjlighet att göra undantag för att gynna viktiga samhälleliga intressen (artikel 44.1 d och 44.5). Vi gör samma bedömning beträffande bestämmelsen om att anställdas tillgång ska begränsas. Bestämmelsen om undantag från informationsskyldigheten på grund av sekretess kan vara kvar som en tillåten komplettering med stöd av möjligheten att göra undantag enligt artikel 21.

Även bestämmelsen om korrigering av en otillåten behandling bedöms kunna utgöra en komplettering till förordningen. I förslaget till förordning förutsätts att var och en ska ha tillgång till ett rättsmedel mot beslut som tillsynsmyndigheten fattar mot vederbörande. Det innebär att den nya lagens bestämmelse om att sådana beslut får överklagas till allmän förvaltningsdomstol utgör en tillåten komplettering av förordningen och alltså kan behållas. Bestämmelsen om överklaganden till allmän förvaltningsdomstol av beslut som en myndighet fattar i egenskap av personuppgiftsansvarig har sin grund i vår inhemska ordning om rätt att överklaga förvaltningsbeslut och är inte att anse som ett utflöde av förordningens bestämmelse om den registrerades rätt att få föra talan i domstol. Den bestämmelsen kan alltså också behållas när förordningen träder i kraft. Detsamma gäller bestämmelsen som klargör att rätten att överklaga regleras uttömmande i den nya lagen.

Bestämmelser som bedöms inte kunna komplettera förordningen

De bestämmelser som reglerar förhållandet till personuppgiftslagen kommer av naturliga skäl inte att kunna kvarstå i lagen, i vart fall inte i oförändrad form.

Den bestämmelse i den nya lagen som anger en generell rättslig grund för myndigheters personuppgiftsbehandling torde inte kunna behållas som ett komplement till förordningen. Bestämmelsen avses i samlad form omfatta de tillämpliga fall enligt artikel 7 i dataskyddsdirektivet när myndigheter får behandla personuppgifter. Artikel 6 i förordningen innehåller en motsvarande reglering och vi bedömer att det inte är möjligt att för alla myndigheter (inom lagens tillämpningsområde) ersätta förordningens rättsliga grunder med en heltäckande nationell reglering som inte anger några närmare specificerade krav än att det ska vara fråga om en behandling som är nödvändig för att en myndighet ska kunna utföra sin verksamhet. Mycket talar således för att bestämmelsen får ersättas med en hänvisning till förordningen. Det är sedan en annan sak att mer specificerade eller avvikande bestämmelser för vissa särskilda verksamheter eller liknande kan tas in som särreglering i förhållande till uppgiftsskyddsförordningen.

Förordningens bestämmelser om säkerhet vid behandling är mycket utförliga och överensstämmer i princip med motsvarande bestämmelser i den nya lagen. Lagens bestämmelser torde därför inte utgöra en tillåten komplettering, frånsett den bestämmelse som anger att myndigheter vid utformning av säkerhetsåtgärder även ska beakta bestämmelser om informationssäkerhet i annan författning som gäller för myndigheten, vilken vi alltså bedömer kan behållas. Vad gäller bestämmelserna om personuppgiftsbiträde i den nya lagen är dessa i stort överensstämmande med förordningens krav och torde därför få upphävas. Med tanke på förordningens bestämmelser i artikel 28 om att registeransvariga ska dokumentera sin behandling bedömer vi att den nya lagens föreskrift om att en förteckning ska föras utgör en med förordningen oförenlig dubbelreglering då den i stor utsträckning torde ställa samma krav. Vad gäller undantaget i den nya lagen från skyldigheten att lämna information på begäran såvitt avser personuppgifter i ostrukturerat material förefaller uppgiftsskyddsförordningen inte öppna för något undantag från informationsskyldigheten enligt artikel 15 annat än med stöd av artikel 21.

Bestämmelsen om rättelse och komplettering av felaktiga eller ofullständiga personuppgifter torde i alltför hög grad sakna självständigt innehåll i förhållande till uppgiftsskyddsförordningen för att den ska kunna anses utgöra en komplettering till förordningen.

I bestämmelsen om korrigering av en otillåten behandling kan i stället en hänvisning till bestämmelsen om rättelse i förordningen göras.

I förordningen regleras på ett uttömmande sätt vilka befogenheter som tillsynsmyndigheten ska ha och vad som ska vara myndighetens uppgifter inom ramen för dess tillsyn. Något utrymme för sådana bestämmelser i nationell lagstiftning torde därför inte finnas.

19.2.3 Konsekvenser för myndighetsverksamhet som inte omfattas av förordningen

Den brottsbekämpande verksamheten omfattas inte av kommissionens förslag till en allmän uppgiftsskyddsförordning utan av ett förslag till ett direktiv. Denna verksamhet, som inte omfattas av vårt uppdrag, föreslår vi ska helt undantas från den nya lagens tillämpningsområde.

Flera myndigheter bedriver emellertid verksamheter som kommer att falla delvis inom den ena, delvis den andra rättsakten. Skatteverket och Tullverket är några exempel.

Givetvis kan man befara vissa problem, inte minst praktiska sådana, för myndigheter med blandade verksamheter som omfattas av olika rättsakter.

Några prognoser rörande den slutliga utformningen och innehållet i direktivet för den brottsbekämpande verksamheten är mycket svåra att göra. Vi ser det således inte som möjligt att föregripa detta genom att nu göra någon bedömning i fråga om möjlig anpassning av bestämmelser i den nya lagen som tar sikte på just myndigheter med ”blandade” personuppgiftsbehandlingar. Dock vill vi framhålla att de materiella bestämmelserna i den nya lagen torde vara så utformade att det inte ska behöva uppkomma någon konflikt i den praktiska informationshanteringen på grund av skillnader mellan bestämmelserna i den nya lagen och den speciella reglering som kan förmodas införas på grundval av direktivet för den brottsbekämpande verksamheten.

När dataskyddsdirektivet genomfördes i svensk rätt gjordes personuppgiftslagen generellt tillämplig. Den gjordes därmed tillämplig också på sådan verksamhet som inte omfattades av den dåvarande EG-rätten, exempelvis statens verksamhet på straffrättens område eller som rör allmän säkerhet eller försvar. Även den nya lagen före-

slås gälla generellt för myndigheters verksamhet med några särskilt utpekade undantag.

Eftersom en blivande uppgiftsskyddsförordning inte ska genomföras i svensk rätt utan blir direkt tillämplig inom sitt område såsom en direkt gällande EU-rättsakt, saknar medlemsstaterna befogenhet att göra förordningen tillämplig på områden som ligger utanför EU-rätten. När förordningen träder i kraft kan den nya lagen därför inte längre gälla generellt för myndigheters behandling av personuppgifter i den del som lagen avser att utgöra en komplettering till förordningen. För att i så hög grad som möjligt bibehålla ett enhetligt regelverk när det gäller myndigheters behandling av personuppgifter bör man i den nya lagen kunna föra in en bestämmelse som föreskriver att myndigheter vars verksamhet inte omfattas av uppgiftsskyddsförordningens tillämpningsområde ska behandla personuppgifter på ett sådant sätt att behandlingen uppfyller de materiella hanteringskrav som följer av förordningen och den nya lagen. I lagen bör också klargöras att registrerade vars personuppgifter behandlas i sådan verksamhet har motsvarande rättigheter i förhållande till svenska myndigheter som de registrerade vars personuppgifter behandlas enligt förordningen. Det kommer också att behövas särskilda bestämmelser om tillsynsmyndighetens befogenheter i förhållande till myndigheter av nu aktuellt slag. Genom en sådan lösning får utveckling av praxis och ändringar i regelverket i princip samma betydelse även för dessa myndigheters personuppgiftsbehandling.

19.3 Enligt kommittéförordning och direktiv

Bedömning: Våra förslag innebär införandet av en samlad och enhetlig reglering av myndigheters behandling av personuppgifter som ger förutsättningar för en mer ändamålsenlig informationshantering inom myndighetssfären. Detta gynnar registrerades integritet, allmänhetens insyn och effektiviteten i den offentliga förvaltningen. Några sådana ekonomiska kostnadsökningar eller övriga konsekvenser som avses i 14–15 a §§ kommittéförordningen finns inte.

Vår uppgift

Enligt våra direktiv gäller att vi ska bedöma de ekonomiska konsekvenserna av förslagen för det allmänna och för enskilda. Om förslagen kan förväntas leda till kostnadsökningar för det allmänna, ska vi föreslå hur dessa ska finansieras. För vårt arbete gäller dessutom bestämmelserna i kommittéförordningen (1998:1474). I 14 § anges att om förslagen i ett betänkande påverkar kostnaderna eller intäkterna för staten, kommuner, landsting, företag eller andra enskilda, ska en beräkning av dessa konsekvenser redovisas i betänkandet. Om förslagen innebär samhällsekonomiska konsekvenser i övrigt, ska dessa redovisas. När det gäller kostnadsökningar och intäktsminskningar för staten, kommuner eller landsting, ska kommittén föreslå en finansiering. Vidare följer av 15 § att förslagens eventuella konsekvenser för den kommunala självstyrelsen ska anges i betänkandet. Detsamma gäller när ett förslag har betydelse för brottsligheten och det brottsförebyggande arbetet, för sysselsättning och offentlig service i olika delar av landet, för små företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt i förhållande till större företags, för jämställdheten mellan kvinnor och män eller för möjligheterna att nå de integrationspolitiska målen. Om ett betänkande innehåller förslag till nya eller ändrade regler, ska, enligt 15 a §, förslagens kostnadsmässiga och andra konsekvenser anges i betänkandet. Konsekvenserna ska anges på ett sätt som motsvarar de krav på innehållet i konsekvensutredningar som finns i 6 och 7 §§ förordningen (2007:1244) om konsekvensutredning vid regelgivning.

Våra överväganden

De föreslagna bestämmelserna i den nya lagen för myndigheters behandling av personuppgifter utgör inga egentliga materiella förändringar för myndigheterna vad gäller när och hur de får behandla personuppgifter i deras verksamheter. Syftet med förslagen är i stället att förenkla för i första hand lagstiftaren och myndigheterna genom att göra regleringen tydligare, enhetligare och bättre anpassad till övrig reglering som styr myndigheternas informationshantering. En långsiktig målsättning är vidare att minska den samlade regel-

massan och underlätta den kommande anpassningen till uppgiftsskyddsförordningen.

Det är vår uppfattning att förslagen som helhet främjar myndigheternas möjligheter att erbjuda bättre offentlig service. Vårt förslag till avreglering av begränsningar i fråga om elektroniskt utlämnande kommer t.ex. att underlätta såväl för allmänhetens insyn i myndigheternas verksamhet som för företag som är s.k. vidareutnyttjare av offentlig information.

De egentliga materiella förändringarna är som redan sagts begränsade och utgör i hög grad tydliggöranden av vad gällande rätt som vi ser det redan kräver av myndigheter när de behandlar personuppgifter sedda i ljuset av andra krav på myndigheters informationshantering som också ska följas. Så är t.ex. fallet, menar vi, med de föreslagna kraven på att myndigheters säkerhetsarbete ska vara processorienterat och omfatta såväl förebyggande som uppföljande åtgärder samt att det ska ske med beaktande av parallella krav på informationssäkerhetsarbete som myndigheterna också måste följa. Andra exempel är kraven på risk- och sårbarhetsanalyser och överenskommelser vid direktåtkomst samt att anställdas tillgång till personuppgifter ska vara behovsanpassad. Den nya regleringen av korrigering av felaktiga personuppgifter respektive annars otillåten behandling hör också till denna kategori.

I övrigt är de materiella förändringarna, tillsammans med att regleringen samlas i en generell lag, ägnade att skapa ett tydligare och mer enhetligt integritetsskydd inom den offentliga verksamheten. Det är alltså vår uppfattning att den samlade effekten bidrar till såväl ett förbättrat integritetsskydd hos myndigheterna som förutsättningar för en bättre servicenivå gentemot medborgarna.

Det är vår bedömning att våra förslag inte medför några förändringar i förutsättningarna för myndigheternas verksamhet som får sådana kostnadsmässiga konsekvenser som avses i 14 § kommittéförordningen och som inte ryms inom myndigheternas ordinarie budgetramar. Inte heller har förslagen några sådana konsekvenser som avses i 15 § eller ska redovisas enligt 15 a § kommittéförordningen.

20 Ikraftträdande och övergångsbestämmelser

Förslag: Den nya lagen liksom lagen om ändring i offentlighets- och sekretesslagen ska träda i kraft den 1 januari 2017.

Om ett avtal om uppdrag som personuppgiftsbiträde har ingåtts före ikraftträdandet gäller 30 § PuL för uppdraget i stället för de nya bestämmelserna under en övergångsperiod om två år från ikraftträdandet.

I fråga om en begäran om korrigering av en felaktig personuppgift eller en otillåten behandling ska 28 § PuL tillämpas i stället för de nya bestämmelserna om begäran har gjorts före ikraftträdandet.

20.1 Myndighetsdatalagen

Tidpunkt för ikraftträdande

Den nya generella lagen för myndigheters behandling av personuppgifter kommer från och med den tidpunkt då lagen träder i kraft att gälla fullt ut för de myndigheter som då behandlar personuppgifter enbart med stöd av personuppgiftslagen. Dessa myndigheter kommer alltså härefter att behandla personuppgifter enbart med stöd av den nya lagen, utom i de fall lagen föreskriver att vissa bestämmelser i personuppgiftslagen ska tillämpas på motsvarande sätt. De frågor som den nya lagen reglerar är väl bekanta för myndigheterna och har i flera avseenden motsvarigheter i personuppgiftslagen. Vad gäller vissa frågor behöver myndigheterna emellertid nödvändig tid för att förbereda sig för den nya lagen. För att möjliggöra nödvändig anpassning och därmed undvika omfattande och detaljerade

övergångsbestämmelser föreslår vi att tidpunkten för ikraftträdandet läggs relativt långt fram i tiden. Vi bedömer därvid att ett halvår från lagens beslutande till dess ikraftträdande ger myndigheterna en rimlig förberedelseperiod. Med den förutsättningen att riksdagen beslutar lagen före sommaruppehållet 2016 bör lagen därför träda i kraft först den 1 januari 2017.

För de myndigheter som vid ikraftträdandet helt eller delvis behandlar personuppgifter med stöd av en eller flera registerförfattningar kommer den nya lagen inte att vara tillämplig i den registerförfattningsreglerade verksamheten. Det beror på att 4 § föreskriver att avvikande bestämmelser i annan lag än personuppgiftslagen eller förordning ska tillämpas i stället för den nya lagen. I den mån sådana registerförfattningar föreskriver att vissa bestämmelser i personuppgiftslagen ska tillämpas vid behandling av personuppgifter enligt registerförfattningen i fråga, ska alltså personuppgiftslagen tillämpas också fortsättningsvis och inte den nya lagen. Detsamma gäller det mera vanliga fallet att registerförfattningen i fråga gäller utöver personuppgiftslagen, vilket brukar anges i registerförfattningen. I vilken utsträckning sådana myndigheter som behandlar personuppgifter med stöd av en registerförfattning i framtiden ska behandla personuppgifter med stöd av den nya lagen beror på om regelverket för respektive myndighet anpassas till den nya lagen och förutsätter att registerförfattningen i fråga i så fall upphävs eller i vart fall ändras.

Vissa registerförfattningar av den typ vi har kallat renodlade registerförfattningar, som t.ex. reglerar ett visst specifikt register, innehåller inte bestämmelser som hänvisar till personuppgiftslagen. I den mån en sådan författning inte reglerar frågor om exempelvis information till den registrerade, rättelse och tillsynsmyndighetens befogenheter, och inte heller bestämmelser i någon annan registerförfattning är tillämpliga, gäller personuppgiftslagen. Sådana frågor kommer således efter den nya lagens ikraftträdande att omfattas av den nya lagens tillämpningsområde.

Behovet av övergångsbestämmelser

Det kan konstateras att den nya lagen i stor utsträckning innebär en mer ändamålsenlig reglering av myndigheters behandling av personuppgifter och i allmänhet inte begränsar myndigheters möjlighet att

behandla personuppgifter i förhållande till personuppgiftslagen. Något generellt behov av att anpassa myndigheternas tekniska system till de förutsättningar som kommer att gälla enligt den nya lagen finns inte. Lagen är genomgående teknikneutral. Även den föreslagna bestämmelsen som förbjuder att känsliga personuppgifter används som sökbegrepp syftar till att sätta upp rättsliga gränser för personuppgiftsbehandlingen. De åtgärder som eventuellt kan behöva vidtas från myndigheternas sida med anledning av den bestämmelsen handlar om praktiska anpassningar genom exempelvis åtkomstbegränsningar, som alltså inte behöver vara av tekniskt slag utan kan bestå i någon form av rättsliga hinder, och att eventuellt rensa vissa informationssamlingar från överflödig information.

I några avseenden innehåller lagen bestämmelser som syftar till att förtydliga vad som ska gälla i jämförelse med reglerna i personuppgiftslagen. Det gäller t.ex. bestämmelserna som rör direktåtkomst. I det sammanhanget föreslås en bestämmelse som klargör att direktåtkomst till sekretessreglerade personuppgifter som huvudregel kräver stöd i lag eller förordning. Det torde höra till undantagsfallen att en myndighet har medgett direktåtkomst till sekretessreglerade personuppgifter utan att det finns bestämmelser om sådan åtkomst i en tillämplig författning. I den mån sådan behandling genom oreglerad direktåtkomst förekommer, och som alltså i det enskilda fallet kan antas fylla ett angeläget verksamhetsbehov, torde det inte vara fråga om några mer omfattande sådana åtkomster och nödvändigt författningsstöd bör kunna ges i form av en bestämmelse i förordning. Behovet av anpassning kan därför tillgodoses inom förberedelseperioden fram till lagens ikraftträdande.

Även i andra fall kan myndigheterna antas behöva viss tid för att anpassa sig till den nya regleringen. Det gäller bl.a. kravet på att personalens tillgång till personuppgifter ska vara behovsanpassad samt de skärpta förutsättningarna för att återge personnummer i beslut. Också i dessa avseenden finns enligt vår bedömning emellertid tillräckligt utrymme för att förbereda sig fram till det föreslagna ikraftträdandet. De föranleder alltså inte något behov av någon ytterligare övergångsperiod.

Den nya lagens uttryckliga krav på att det bl.a. ska göras en risk- och sårbarhetsanalys innan en myndighet medger direktåtkomst till personuppgifter eller ett integrerat informationssystem tas i bruk föranleder inte heller något behov av en ytterligare övergångsperiod.

Detsamma kan sägas om skyldigheten att föra en förteckning över personuppgiftsbehandlingar.

Den nya lagen innebär att undantagsbestämmelsen i 5 a § PuL om att vissa bestämmelser i lagen inte behöver tillämpas på personuppgifter som ingår i ostrukturerade uppgiftssamlingar inte gäller för myndigheter. Som vårt förslag har utformats gör vi bedömningen att bestämmelsen inte i något fall behövs för att tillåta en behandling av personuppgifter (se avsnitt 8.3.2.). Någon övergångsperiod på grund av att 5 a § PuL inte längre ska gälla för myndigheter behövs därför inte.

Enligt vår bedömning behövs särskilda övergångsbestämmelser endast för två fall. Det första fallet gäller de krav som enligt lagen ställs på en myndighet som anlitar ett personuppgiftsbiträde om vad ett skriftligt avtal om uppdrag som personuppgiftsbiträde ska innehålla. Den regleringen bör endast gälla för sådana avtal som ingås efter det att lagen har trätt i kraft. Det är dock enligt vår mening rimligt att omförhandling av långvariga uppdrag ska ha skett senast inom två år från lagens ikraftträdande. För ett avtal om uppdrag som personuppgiftsbiträde som redan har träffats vid lagens ikraftträdande bör alltså personuppgiftslagens bestämmelser gälla i stället fram till och med den 31 december 2018. Vidare bör i fråga om en begäran om korrigering av en felaktig eller otillåten behandling av personuppgifter som gjorts före ikraftträdandet 28 § PuL tillämpas i stället för 24 och 25 §§, eftersom bestämmelserna i den nya lagen innebär vissa begränsningar i den registrerades rätt i förhållande till vad som gäller enligt personuppgiftslagen.

20.2 Lagen om ändring i offentlighets- och sekretesslagen

Den nya bestämmelsen som föreslås införas i 10 kap. 28 § OSL, som innebär att bestämmelser om direktåtkomst i lag eller förordning i sig är sekretessbrytande, bör träda i kraft vid samma tidpunkt som den nya lagen, dvs. den 1 januari 2017. Ändringen påverkar inte sekretessbrytande bestämmelser som redan meddelats för att möjliggöra en viss direktåtkomst. Däremot innebär ändringen att det för framtida bestämmelser om tillåten direktåtkomst ställs krav på att bestämmelserna har en sådan konkretion att det går att läsa ut vilka

personuppgifter som kan lämnas ut genom åtkomsten utan hinder av sekretess.

21 Författningskommentar

21.1 Förslaget till myndighetsdatalag

Lagens syfte och tillämpningsområde

1 § Syftet med denna lag är att ge myndigheter möjligheter att behandla personuppgifter på ett ändamålsenligt sätt i deras verksamheter och att skydda människor mot att deras personliga integritet kränks vid sådan behandling.

I paragrafen anges lagens övergripande syfte. Frågan behandlas i avsnitt 8.1.2.

Syftet med lagen är tudelat. Lagen ska både ge myndigheter möjligheter att behandla personuppgifter på ett ändamålsenligt sätt och skydda människor mot att deras personliga integritet kränks vid sådan behandling. Därmed tydliggörs bl.a. att personuppgiftsbehandling som kan anses utgöra intrång i enskildas personliga sfär alltid måste stå i rimlig proportion till samhällets behov. Paragrafen är en portalbestämmelse som i första hand har en informativ och pedagogisk betydelse då den klargör den övergripande målsättningen med regleringen, vilken är att reglera informationshanteringen i förhållande till det behov av dataskydd som myndigheters personuppgiftsbehandling påkallar. Paragrafen är även avsedd att kunna ge vägledning för hur materiella bestämmelser i lagen bör tolkas i tveksamma fall.

2 § Denna lag gäller vid myndigheters behandling av personuppgifter.

Lagen gäller om behandlingen är helt eller delvis automatiserad eller om personuppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

Paragrafen anger lagens tillämpningsområde. Frågan behandlas i avsnitt 8.2.1 (första stycket) och 8.2.4 (andra stycket).

I *första stycket* anges att lagen gäller myndigheters behandling av personuppgifter. Med myndigheter avses detsamma som i regeringsformen, dvs. alla statliga och kommunala organ utom riksdagen och de beslutande kommunala församlingarna. Det betyder att lagen som utgångspunkt omfattar regeringen, domstolarna och alla statliga eller kommunala förvaltningsmyndigheter (jfr 1 kap. 8 § RF). Kommunala bolag m.m. som avses i 2 kap. 3 § OSL omfattas inte. Tillämpningsområdet begränsas dock genom dels föreskrivna undantag för vissa verksamheter hos myndigheterna, dels det förhållandet att lagen är subsidiär till annan reglering. Begreppen behandling respektive personuppgift används med samma innebörd som i 3 § PuL. Med behandling avses således varje åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter. Insamling, registrering, organisering, lagring, bearbetning eller ändring, återvinning, inhämtande, användning, utlämnande genom översändande, spridning eller annat tillhandahållande av uppgifter, sammanställning eller samkörning, blockering, utplåning eller förstöring är behandling. Sådana åtgärder beträffande personuppgifter som regleras i lagen, exempelvis avskiljande, är ytterligare exempel på behandling. Begreppet personuppgift omfattar all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet. Behandling av uppgifter om avlidna omfattas således inte av lagen. Detsamma gäller uppgifter om juridiska personer. Om bestämmelser om behandling av personuppgifter på något visst område bör vara tillämpliga även beträffande uppgifter om avlidna eller juridiska personer får detta föreskrivas särskilt.

Genom *andra stycket* klargörs att inte all slags behandling av personuppgifter omfattas av lagens tillämpningsområde. Det krävs att behandlingen är helt eller delvis automatiserad eller att personuppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier. Rekvisiten är desamma som i artikel 2 c och 3.1 i dataskyddsdirektivet respektive 5 § PuL och ska ha motsvarande innebörd. Helt manuell behandling av personuppgifter som inte ingår i ett register eller annan samling som är tillgänglig för sökning faller därmed utanför lagens tillämpningsområde. I praktiken torde dock endast en ytterst liten del av personuppgiftsbehandlingen inom den offentliga sektorn vara helt manuell.

3 § Lagen ska inte tillämpas vid behandling av personuppgifter i
1. en myndighets administrativa verksamhet,
2. en myndighets verksamhet som personuppgiftsbiträde, eller
3. den verksamhet som bedrivs av behöriga myndigheter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller beivra brott eller verkställa straffrättsliga påföljder.

I paragrafen anges tre uttryckliga undantag från lagens tillämpningsområde. Undantagen är knutna till vissa slags verksamheter hos myndigheter. Frågan behandlas i avsnitt 8.2.2.

Punkten 1 kan sägas beröra alla myndigheter som i övrigt tillämpar lagen. Det undantagna området enligt denna punkt avser myndigheters administrativa verksamhet. Med den verksamheten förstås sådana från myndigheternas sakområden åtskilda aktiviteter som att anställa och avlöna personal, införskaffa kontorsmaterial, lokalfrågor, fakturahantering och liknande renodlade ekonomi- eller personaladministrativa göromål inom en myndighet. Den personuppgiftsbehandling som sker i sådan administration av internt slag omfattas inte av lagens tillämpningsområde utan regleras av personuppgiftslagen. Undantaget omfattar dock inte sådan mer övergripande planering, uppföljning och kontroll och annan administration som är direkt kopplad till en myndighets sakverksamhet. Uppkommer behov av behandling av personuppgifter som samlats in i sakverksamheten, exempelvis för att få fram viss statistik som behövs i den egna verksamhetsplaneringen eller kvalitetssäkringen, omfattas alltså även den behandlingen av lagen.

Enligt *punkten 2* är lagen inte tillämplig vid behandling av personuppgifter som en myndighet utför i egenskap av personuppgiftsbiträde åt en annan myndighet eller en enskild som är personuppgiftsansvarig. Med begreppen personuppgiftsbiträde och personuppgiftsansvarig avses detsamma som i personuppgiftslagen (3 § PuL). Lagen omfattar alltså bara myndigheter när de är personuppgiftsansvariga. Vad som gäller för en behandling som en myndighet genomför som personuppgiftsbiträde beror alltså på vilken reglering som gäller för den personuppgiftsansvarige. Lagen kan således bli indirekt tillämplig hos en myndighet som är personuppgiftsbiträde, nämligen om den personuppgiftsansvarige uppdragsgivaren är en myndighet vars behandling regleras av lagen. I ett sådant fall är det dock alltid den personuppgiftsansvariga myndigheten som bär an-

svaret för att behandlingen hos biträdesmyndigheten sker enligt lagen. Det ska observeras att undantaget inte omfattar myndigheter som utan att vara personuppgiftsbiträde behandlar personuppgifter för sådan teknisk lagring eller bearbetning som avses i 2 kap. 10 § första stycket TF. Det krävs alltså att det finns ett giltigt personuppgiftsbiträdesavtal för att undantaget ska gälla.

I *punkten 3* undantas den s.k. brottsbekämpande verksamheten från lagens tillämpningsområde. Med brottsbekämpande verksamhet avses verksamhet för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller beivra brott eller verkställa straffrättsliga påföljder. Denna beskrivning överensstämmer i sak med motsvarande undantag i dataskyddsdirektivet och i kommissionens förslag till uppgiftsskyddsförordning. Undantaget omfattar enbart verksamhet hos myndigheter som har till särskild uppgift att bedriva verksamhet av nämnt slag. Vilka myndigheter som har sådana uppgifter framgår framför allt av myndighetsinstruktioner, verksamhetsreglering eller av särskilda regeringsuppdrag. Undantaget torde bara träffa statliga myndigheter, varav flertalet omfattas av gällande eller föreslagna informationshanteringsförfattningar. Polismyndigheten, Ekobrottsmyndigheten, Åklagarmyndigheten och Kriminalvården är uppenbara exempel på myndigheter med behörighet att bedriva verksamhet som omfattas av undantaget i punkten 3. De allmänna domstolarna, Skatteverket, Tullverket och Kustbevakningen har också uppgifter inom sådan verksamhet. För flertalet av de nämnda myndigheterna gäller att undantaget inte träffar alla delar av myndighetens verksamhet. Exempelvis har Polismyndigheten en rad ytterligare uppgifter vid sidan om brottsbekämpningen. Om dessa andra delar regleras av lagen eller inte beror på i vilken utsträckning det finns särreglering som i så fall gäller framför lagen eftersom den är subsidiär till annan reglering i lag eller förordning, se 4 §. Det finns ytterligare myndigheter än de nämnda som har tämligen avgränsade uppgifter inom brottsbekämpningen vilken torde medföra viss personuppgiftsbehandling som omfattas av undantaget, exempelvis den verksamhet hos Bolagsverket och Finansinspektionen som följer av lagen (2009:62) om åtgärder mot penningtvätt och finansiering av terrorism med anknytande förordning eller verksamhet hos Statens institutionsstyrelse enligt lagen (1998:603) om verkställighet av sluten ungdomsvård som är en straffrättslig påföljd. Däremot träffar undantaget inte sådan personuppgiftsbehandling som kan äga rum

hos en stor mängd myndigheter på grund av en författningsreglerad skyldighet att anmäla brott till Polismyndigheten eller att annars lämna uppgifter till brottsbekämpande myndigheter. Sådana föreskrifter om uppgiftslämnande innebär inte en behörighet, dvs. en särskild uppgift, att bedriva brottsbekämpande verksamhet, vilket är en förutsättning för att undantaget ska vara tillämpligt.

Förhållandet till annan författning

4 § Om det i en annan lag eller förordning än som avses i 5 § finns bestämmelser som avviker från denna lag, ska de bestämmelserna gälla.

Paragrafen reglerar lagens förhållande till bestämmelser i annan författning som avviker från innehållet i lagen. Frågan behandlas i avsnitt 8.2.3.

Av paragrafen följer att lagen är subsidiär till avvikande reglering i annan lag eller förordning som rör verksamheter som inte redan undantagits från lagens tillämpningsområde. Sådana avvikande bestämmelser finns framför allt i s.k. registerförfattningar som reglerar inrättandet och förandet av viktigare register på det offentliga området eller annars innehåller bestämmelser om behandling av personuppgifter som myndigheter ska eller får utföra. Även bestämmelser som föreskriver att myndigheter får eller ska lämna ut uppgifter avses i paragrafen. Frågan om en viss bestämmelse innefattar en avvikelse från vad som ska gälla enligt lagen får avgöras med tillämpning av sedvanliga metoder för tolkning av författningar (jfr prop. 1997/98:44 s. 116). I den utsträckning en lag eller förordning med i övrigt avvikande bestämmelser inte innehåller bestämmelser i en fråga som regleras i denna lag, ska denna lags bestämmelser tillämpas, om det inte klart framgår av den särskilda lagen eller förordningen att det är personuppgiftslagens bestämmelser som ska tillämpas i ett sådant fall. Så kan vara fallet om det i den särskilda lagen anges att det är personuppgiftslagen som ska tillämpas, om inte annat följer av registerförfattningen i fråga (se t.ex. 2 § lagen [2002:546] om behandling av personuppgifter i den arbetsmarknadspolitiska verksamheten och 114 kap. 6 § SFB). Lagens subsidiaritet gäller dock inte i förhållande till personuppgiftslagen eller personuppgiftsförordningen. Detta följer av hänvisningen till 5 §.

5 § Om inte annat anges i 6 § gäller denna lag i stället för personuppgiftslagen (1998:204) eller föreskrifter som meddelats i anslutning till den lagen.

I paragrafen regleras lagens förhållande till personuppgiftslagen. Frågan behandlas i avsnitt 8.3.2.

Av paragrafen följer att lagen ersätter personuppgiftslagen och föreskrifter som har meddelats i anslutning till personuppgiftslagen, dvs. personuppgiftsförordningen samt tillsynsmyndighetens föreskrifter som meddelats med stöd av den förordningen. Vid behandling av personuppgifter enligt lagen ska personuppgiftslagen och föreskrifter som meddelats i anslutning till personuppgiftslagen tillämpas endast i den utsträckning som det särskilt anges i lagen. I 6 § finns bestämmelser som hänvisar till bestämmelser i personuppgiftslagen som ska vara tillämpliga även vid personuppgiftsbehandling enligt lagen.

6 § Följande bestämmelser i personuppgiftslagen (1998:204) ska tillämpas på motsvarande sätt när personuppgifter behandlas enligt denna lag eller föreskrifter som meddelats med stöd av den:

1. 3 § om definitioner,

2. 8 § om förhållandet till offentlighetsprincipen m.m.,

3. 9 § om grundläggande krav på behandlingen,

4. 13, 15, 16, 18 och 19 §§ om känsliga personuppgifter,

5. 23 och 25 §§ om information till den registrerade som ska lämnas självmant,

6. 26 § om information till den registrerade som ska lämnas efter ansökan,

7. 33–35 §§ om överföring av personuppgifter till tredjeland,

8. 38 och 40 §§ om personuppgiftsombud, och

9. 48 § om skadestånd.

I 23 § finns bestämmelser om undantag från informationsskyldigheten enligt första stycket 5 och 6.

I paragrafen hänvisas till bestämmelser i personuppgiftslagen som ska tillämpas på motsvarande sätt vid behandling av personuppgifter enligt lagen. Frågorna behandlas dels översiktligt i avsnitt 8.3.2, dels specifikt beträffande de särskilda hänvisningarna i det nämnda avsnittet (3 § och 8 § första stycket PuL), i avsnitt 9.2.4 (9 § PuL),

avsnitt 9.3.1 (13, 15, 16, 18 och 19 §§ PuL), avsnitt 12.5 (33–35 §§ PuL), avsnitt 13.4 (23, 25 och 26 §§ PuL), avsnitt 14.4.2 (8 § andra stycket PuL), avsnitt 16.4.2 (38 och 40 §§ PuL) samt avsnitt 18.1.5 (48 § PuL).

I första stycket anges i nio punkter vilka bestämmelser i personuppgiftslagen som ska tillämpas vid behandling enligt den nya lagen som, enligt vad som föreskrivs i 5 §, i övrigt ersätter personuppgiftslagen. Uppräkningen är uttömmande. I bestämmelsen anges att tillämpningen av hänvisade bestämmelser ska ske ”på motsvarande sätt”. Härmed tydliggörs att de uppräknade bestämmelserna i personuppgiftslagen inte tillämpas direkt. Innebörden av hänvisningen är att vad som föreskrivs i de hänvisade bestämmelserna i personuppgiftslagen ska tillämpas som om motsvarande bestämmelser fanns i den nya lagen. Se nedan angående punkterna 2 och 9.

Enligt *punkten 1* ska de definitioner som anges i 3 § PuL tillämpas även vid behandling av personuppgifter som omfattas av den nya lagen. Genom 3 § PuL definieras bl.a. följande begrepp: behandling (av personuppgifter), mottagare, personuppgifter, personuppgiftsansvarig, personuppgiftsbiträde, personuppgiftsombud, den registrerade, samtycke, tillsynsmyndighet och tredjeland.

Genom hänvisningen i *punkten 2* till 8 § PuL klargörs till en början att bestämmelserna i förevarande lag eller föreskrifter som meddelats i anslutning till lagen, liksom de bestämmelser i personuppgiftslagen som lagen hänvisar till, inte ska tillämpas om de skulle inskränka en myndighets skyldighet enligt 2 kap. TF att lämna ut personuppgifter i allmänna handlingar (8 § första stycket PuL). Det innebär t.ex. att bestämmelserna i personuppgiftslagen och i förevarande lag om under vilka begränsade förutsättningar känsliga personuppgifter får behandlas inte kan åberopas för att vägra behandla uppgifterna genom att lämna ut en allmän handling där känsliga personuppgifter förekommer. Det ska dock observeras att hänvisningen till 8 § första stycket inte innebär någon inskränkt räckvidd av regler om absoluta sökbegränsningar som finns i 12 § eller kan komma att föreskrivas i anslutning till lagen. Sådana omfattas alltså av begränsningsregeln i 2 kap. 3 § tredje stycket TF. Av hänvisningen till 8 § andra stycket PuL följer att varken de särskilda bestämmelserna i den förevarande lagen eller bestämmelser i personuppgiftslagen som ska tillämpas på motsvarande sätt hindrar att allmänna handlingar som innehåller personuppgifter arkiveras och bevaras eller tas

om hand av arkivmyndighet för fortsatt långtidsbevarande i enlighet med arkivlagstiftningens reglering. Vidare framgår att 9 § fjärde stycket PuL inte gäller för en myndighets användning av personuppgifter i allmänna handlingar.

Enligt *punkten 3* gäller de grundläggande kraven i 9 § PuL även vid behandling av personuppgifter enligt den nya lagen. De grundläggande kraven i 9 § PuL behandlas tämligen ingående i avsnitt 9.2.1, 9.2.3 och 9.2.4. Det är den personuppgiftsansvariga myndigheten som ska se till att personuppgifter behandlas enbart om det är lagligt och att de behandlas på ett korrekt sätt och i enlighet med god sed (9 § första stycket a och b PuL). Hänvisningen innebär vidare att den personuppgiftsansvariga myndigheten ansvarar för att personuppgifter samlas in bara för särskilda, uttryckligt angivna och berättigade ändamål (9 § första stycket c PuL). Det är vidare den personuppgiftsansvariga myndigheten som – inom ramen för sitt författningsreglerade eller på annat sätt bestämda uppdrag – har att närmare specificera för vilket eller vilka ändamål personuppgifter behandlas i verksamheten. Alltför vida ändamålsbestämningar är inte tillåtna eftersom de inte lever upp till kravet på att vara särskilda. Genom hänvisningen gäller dessutom att personuppgifter inte får behandlas för ett ändamål som är oförenligt med det ändamål för vilket de samlades in (9 § första stycket d PuL). Detta är ett uttryck för den s.k. finalitetsprincipen. Genom bestämmelsen uppställs en begränsning i fråga om huruvida uppgifter som redan finns i verksamheten får behandlas för nya ändamål. Behandling i form av utlämnanden till andra myndigheter eller enskilda ska anses förenliga med ursprungliga ändamål så länge utlämnandena som sådana sker i överensstämmelse med lag, t.ex. offentlighets- och sekretesslagen, eller förordning enligt vilken uppgifterna får eller ska lämnas ut. I praktiken innebär detta att tillämpningen av finalitetsprincipen, som den uttrycks i 9 § första stycket d PuL, för myndigheternas del framför allt torde handla om att göra bedömningar av om myndighetens önskemål om att själv använda uppgifter i de egna informationssamlingarna för ett nytt ändamål är eller inte är oförenligt med de angivna syften som fanns vid insamlingstidpunkten. Generellt gäller att behandling av personuppgifter för historiska, statistiska eller vetenskapliga ändamål inte ska anses som oförenliga med de ändamål för vilka uppgifterna samlades in (9 § andra stycket PuL). Hänvisningen till 9 § PuL innebär också att myndigheten ska se till att de be-

handlade personuppgifterna är adekvata och relevanta i förhållande till ändamålen för behandlingen, att inte fler personuppgifter behandlas än som är nödvändigt med hänsyn till ändamålen för behandlingen, att de behandlade personuppgifterna är riktiga och, om det är nödvändigt, aktuella (9 § första stycket e–g). Härigenom sätts kvalitativa och kvantitativa gränser för vilka personuppgifter som får behandlas. Är det exempelvis tillräckligt för att en arbetsuppgift ska kunna utföras på ett tillfredsställande sätt att bara använda personuppgifter som indirekt går att härleda till enskilda personer, är det i linje med de grundläggande kraven att så sker. Vidare är den personuppgiftsansvariga myndigheten skyldig att självmant vidta alla rimliga åtgärder för att t.ex. rätta sådana personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålen med behandlingen (9 § första stycket h PuL). Sådana åtgärder får dock inte strida mot annan reglering om dokumentationskrav eller liknande eller krav på bevarande av allmänna handlingar. Korrigering på begäran av den registrerade regleras i 24 och 25 §§ denna lag. Slutligen innebär hänvisningen att personuppgiftslagens bestämmelser rörande bevarande av uppgifter ska tillämpas på personuppgifter som inte finns i allmänna handlingar. Således gäller som huvudregel beträffande sådana personuppgifter att uppgifterna inte får bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen (9 § första stycket i PuL). Personuppgifter får dock bevaras för historiska, statistiska eller vetenskapliga ändamål så länge som behövs för dessa ändamål (9 § tredje stycket PuL). Bevarande av personuppgifter som inte ingår i allmän handling för sådana ändamål torde emellertid innebära att de i och med den användningen får anses omhändertagna för arkivering och därmed kommer att utgöra allmän handling.

Genom *punkten 4* blir personuppgiftslagens förbud mot behandling av känsliga personuppgifter tillämpligt även enligt förevarande lag. Det är också genom hänvisningen till 13 § PuL som det framgår vad som är känsliga personuppgifter. Genom punkten 4 görs vidare flertalet av personuppgiftslagens undantag från förbudet mot behandling av känsliga personuppgifter tillämpliga vid myndigheters personuppgiftsbehandling enligt denna lag. Det ska emellertid observeras att även om ett undantag är tillämpligt, måste behandlingen dessutom vara tillåten enligt 8 § denna lag samt uppfylla de grundläggande kraven enligt 9 § PuL. Undantaget enligt 15 § PuL avser

det förhållandet att den registrerade uttryckligen samtycker till behandlingen eller på ett tydligt sätt offentliggjort uppgiften. Vad avser samtycket ska det, förutom att vara uttryckligt, också uppfylla kriterierna på samtycke enligt 3 § PuL, dvs. vara en frivillig, särskild och otvetydig viljeyttring som föregåtts av information om behandlingen. Övriga tillämpliga undantag gäller vissa mer specifika verksamheter eller situationer och torde inte få någon omfattande eller generell tillämpning för myndigheterna vid behandling enligt denna lag. I 10 § finns bestämmelser om ytterligare undantag.

Punkten 5 hänvisar till 23 och 25 §§ PuL vari regleras den personuppgiftsansvariga myndighetens skyldighet att självmant lämna information om behandlingen till den registrerade i samband med att uppgifter samlas in från denne. Informationen ska innehålla de uppgifter som anges i 25 § första stycket PuL. Ett viktigt undantag från informationsskyldigheten följer av 25 § andra stycket samma lag enligt vilket information inte behöver lämnas om sådant som den registrerade redan känner till. Så kan ofta förutsättas vara fallet, t.ex. då en registrerad själv gör en ansökan till en myndighet vilken leder till viss dokumentation m.m. i myndighetens handläggning av ärendet eller då en enskild kontaktar myndigheter via e-post. I andra fall kan det vara mindre troligt att den registrerade redan känner till informationen. Vad som kan antas i olika fall får dock bedömas utifrån vad som förefaller naturligt med tanke på förhållandena i den särskilda verksamheten i fråga m.m. Undantag från informationsplikten gäller vidare vid sekretess som gäller gentemot den registrerade, se 23 § första stycket denna lag.

Enligt *punkten 6* gäller 26 § PuL om information som på begäran ska ges till den registrerade. Av detta följer att det krävs en egenhändigt undertecknad ansökan av den registrerade och att rätten till information är begränsad till en gång per kalenderår. Även denna skyldighet för myndigheter, och den registrerades rätt i motsvarande mån, är begränsad om sekretess gäller gentemot den registrerade, se kommentaren till 23 § första stycket. Dessutom behöver det inte ges någon information om personuppgifter som finns i s.k. ostrukturerat material, se kommentaren till 23 § andra stycket.

I *punkten 7* hänvisas till personuppgiftslagens bestämmelser om överföring till tredjeland, 33–35 §§ PuL. Därmed gäller förbudet enligt 33 § PuL att överföra personuppgifter till tredjeland om landet inte har en adekvat nivå för skyddet av personuppgifter. Frågan om

en skyddsnivå är adekvat ska bedömas med hänsyn till samtliga omständigheter som har samband med överföringen. Särskild vikt ska fästas vid uppgifternas art, ändamålet med behandlingen, hur länge behandlingen ska pågå, ursprungslandet, det slutliga bestämmelselandet och reglerna för behandlingen i tredjeland. Enligt 34 § PuL får uppgifter trots förbudet överföras dels om den registrerade har lämnat sitt samtycke till överföringen, dels om överföringen är nödvändig med hänsyn till vissa uppräknade omständigheter. Det är också enligt den paragrafen tillåtet att föra över personuppgifter för användning enbart i en stat som har anslutit sig till Europarådets dataskyddskonvention. Genom 35 § PuL bemyndigas regeringen, eller i vissa fall den myndighet regeringen bestämmer, att meddela föreskrifter om ytterligare undantag. Sådana undantag finns för närvarande i 12–14 §§ PuF samt i anslutande bilagor. Genom hänvisningen till 35 § PuL framgår att dessa föreskrifter, samt i förekommande fall även tillsynsmyndighetens föreskrifter, gäller även vid behandling enligt denna lag. Vidare gäller att regeringen, eller efter vidarebemyndigande tillsynsmyndigheten, kan besluta om undantag i enskilda fall, 35 § tredje stycket PuL. Ytterligare undantag från förbudet mot överföring till tredjeland finns i 16 § denna lag.

Enligt *punkten 8* gäller bestämmelserna i 38 och 40 §§ PuL om personuppgiftsombudets uppgifter. Ett personuppgiftsombud har dock inte motsvarande skyldighet som enligt 39 § PuL att föra en förteckning över den personuppgiftsansvariga myndighetens behandlingar. Den skyldigheten åvilar enligt denna lag den personuppgiftsansvariga myndigheten, se 22 §. Det är inte obligatoriskt för myndigheter att utse personuppgiftsombud. Det finns inget som hindrar att en myndighet utser flera personuppgiftsombud eller att en person är personuppgiftsombud åt flera myndigheter som exempelvis samarbetar i ett avgränsat e-förvaltningssystem.

Genom hänvisningen i *punkten 9* till 48 § PuL regleras den registrerades rätt till skadestånd. Genom att 48 § PuL ska tillämpas på ”motsvarande sätt” klargörs att rätten till skadestånd är vidare än vad som föreskrivs i 48 § PuL. Rätt till skadestånd kan således uppkomma på grund av behandling i strid med både särskilda bestämmelser i denna lag och mot bestämmelser i personuppgiftslagen som denna lag hänvisar till. Den registrerades rätt till skadestånd omfattar ersättning för skada eller för kränkning av den personliga integriteten. Med skada kan avses personskada, sakskada eller ren

förmögenhetsskada. Det krävs dock att den lagstridiga behandlingen orsakat skadan eller kränkningen. Eventuellt skadestånd beräknas utifrån de allmänna bestämmelserna i 5 kap. SkL. Det är den personuppgiftsansvariga myndigheten som har det skadeståndssanktionerade ansvaret för att behandling av personuppgifter utförs i enlighet med lagens krav. Talan om skadestånd måste emellertid riktas mot den juridiska person, dvs. staten, landstinget eller kommunen, i vilken den personuppgiftsansvariga myndigheten ingår. Hänvisningen innebär att jämkningsregeln i 48 § andra stycket PuL i princip är tillämplig även på myndighetsområdet.

Andra stycket i paragrafen innehåller en upplysning om att det i 23 § finns bestämmelser om undantag från informationsskyldigheten enligt 23, 25 och 26 §§ PuL, se kommentaren till 23 §.

Personuppgiftsansvar

7 § En myndighet är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför.

Personuppgiftsansvaret enligt första stycket omfattar även behandling som en myndighet utför genom direktåtkomst till personuppgifter hos en annan myndighet eller enskild.

Paragrafen innehåller bestämmelser om personuppgiftsansvar. Frågan behandlas i avsnitt 10.1.4.

Bestämmelsen i *första stycket* kompletterar definitionen i 3 § PuL av begreppet personuppgiftsansvarig, enligt vilken det är den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för personuppgiftsbehandlingen som är personuppgiftsansvarig. Innebörden av personuppgiftsansvaret framgår av lagens övriga bestämmelser och av de bestämmelser i personuppgiftslagen som denna lag hänvisar till. Genom bestämmelsen klargörs att personuppgiftsansvaret ligger hos myndigheten, inte hos den juridiska person som myndigheten är en del av. Vidare anges att en myndighet är personuppgiftsansvarig för den behandling som myndigheten utför. Med detta menas att en myndighet ansvarar för den personuppgiftsbehandling som sker inom ramen för myndighetens verksamhet. Personuppgiftsansvaret knyts därmed till utförandet av urskiljbara personuppgiftsbehandlingar. Hos vem personuppgifts-

ansvaret ska förläggas och hur det ska avgränsas får bedömas utifrån de faktiska omständigheterna i det särskilda fallet, där en central fråga är vem som har faktisk möjlighet att påverka om en viss behandling ska ske och hur den ska gå till. En personuppgiftsansvarig myndighet anses utföra en behandling även om den faktiska hanteringen av personuppgifter överlämnats till ett personuppgiftsbiträde. Bestämmelsen utesluter inte att en myndighet kan ha ett med andra myndigheter eller enskilda gemensamt personuppgiftsansvar.

Genom bestämmelsen i *andra stycket* förtydligas att personuppgiftsansvaret enligt första stycket även omfattar sådan behandling som en mottagande myndighet utför när den vid direktåtkomst hos en annan myndighet eller enskild utnyttjar en möjlighet att via direktåtkomst genom faktisk överföring behandla en tillgänglig personuppgift, t.ex. genom att göra en sökning för att läsa eller ladda ned uppgiften till det egna informationssystemet. Huvudregeln i första stycket gäller alltså även vid direktåtkomst. Detta innebär bl.a. att det är den utlämnande myndigheten som har personuppgiftsansvaret för den behandling som myndigheten utför genom det initiala utlämnandet av personuppgifterna då direktåtkomsten faktiskt etableras. Däremot ansvarar alltså denna myndighet inte för den behandling som därefter utförs av en mottagande myndighet.

När behandling kan tillåtas

8 § Personuppgifter får behandlas om det är nödvändigt för att en myndighet ska kunna utföra sin verksamhet.

I paragrafen regleras när behandling av personuppgifter är tillåten. Frågan behandlas i avsnitt 9.2.4.

I bestämmelsen anges en heltäckande rättslig grund för myndigheters behandling av personuppgifter. Bestämmelsen motsvarar i sakligt hänseende de rättsliga grunderna för behandling utan den registrerades samtycke enligt 10 § a–f PuL. Enligt bestämmelsen krävs, för att en myndighet alls ska få behandla personuppgifter, dels att det sker i en verksamhet som myndigheten ska eller har befogenhet att bedriva, dels att personuppgiftsbehandlingen är nödvändig för att den verksamheten ska kunna bedrivas. Vad myndigheter ska eller har befogenhet att göra styrs i allt väsentligt genom

författningsreglering eller särskilda beslut. Inom den gräns som därvid sätts – dvs. om det är en verksamhet som myndigheten ska eller får bedriva – får myndigheter enligt bestämmelsen behandla personuppgifter oberoende av den registrerades samtycke. Dock krävs att personuppgiftsbehandlingen är nödvändig för verksamheten. Myndigheten ska alltså inför en planerad behandling, t.ex. i ett utvecklingsprojekt, först ställa sig frågan om behandlingen kommer att ske som en del i en verksamhet som myndigheten ska eller har getts befogenhet att bedriva. Därefter uppkommer frågan om det är nödvändigt att behandla personuppgifter i projektet. Behövs inte personuppgifterna eller kan en arbetsuppgift utföras nästan lika bra eller billigt utan behandling av personuppgifter är nödvändighetskravet inte uppfyllt och behandlingen därmed inte tillåten (jfr SOU 1997:39 s. 359).

9 § Behandling som är tillåten enligt denna lag eller föreskrifter som meddelats med stöd av den får utföras även om den registrerade motsätter sig behandlingen.

I paragrafen regleras frågan om den enskilde har någon möjlighet att med rättslig verkan motsätta sig behandlingen. Frågan har behandlats i avsnitt 9.2.4.

Enligt paragrafen får en personuppgiftsbehandling, som är tillåten enligt lagen, utföras även om den enskilde motsätter sig den. Bestämmelsen ska ses mot bakgrund av artikel 14 a dataskyddsdirektivet, som föreskriver att den enskilde åtminstone i vissa fall ska garanteras en rätt att motsätta sig en personuppgiftsbehandling, om inte annat föreskrivs i nationell lagstiftning.

Särskilda kategorier av personuppgifter

10 § Utöver vad som följer av 15, 16, 18 och 19 §§ personuppgiftslagen (1998:204) får känsliga personuppgifter behandlas om uppgifterna har lämnats i ett ärende eller är nödvändiga för handläggningen av det eller om uppgifterna behandlas endast i löpande text.

I paragrafen anges i vilken utsträckning känsliga personuppgifter får behandlas. Frågan behandlas i avsnitt 9.3.1.

Enligt *första stycket* får känsliga personuppgifter behandlas i viss utsträckning utöver de särskilda undantag från förbudet i 13 § PuL som regleras i 15, 16, 18 och 19 §§ samma lag. Att 13, 15, 16, 18 och 19 §§ PuL tillämpas på motsvarande sätt när personuppgifter behandlas enligt denna lag eller föreskrifter som meddelats med stöd av den framgår av 6 § första stycket 4. Med känsliga personuppgifter avses således detsamma som enligt 13 § PuL. Utöver de nämnda särskilda undantagen som gäller enligt personuppgiftlagen får känsliga personuppgifter behandlas om uppgifterna har lämnats i ett ärende. Något krav på att det är nödvändigt att behandla uppgiften i ärendet uppställs inte i det fallet. Det är således tillåtet att även på automatiserad väg behandla känsliga personuppgifter som exempelvis en enskild har lämnat i en inlaga i ett ärende, även om uppgiften inte är nödvändig för att myndigheten ska kunna handlägga ärendet. Om myndigheten av något annat skäl behöver behandla en känslig personuppgift, exempelvis för att den själv samlat in uppgiften, krävs emellertid att uppgiften är nödvändig för handläggningen av ett ärende. Det är tillåtet att behandla en känslig personuppgift så länge den är nödvändig för handläggningen av ett ärende, oavsett på vilket sätt behandlingen sker. Om den förutsättningen är uppfylld, ger bestämmelsen således stöd för att exempelvis hantera känsliga personuppgifter inom ramen för ett ärendehanteringssystem.

Känsliga personuppgifter kan vidare med stöd av paragrafen behandlas i verksamhet som inte innebär handläggning av ett ärende om det sker i löpande text. Något krav på nödvändighet uppställs inte, eftersom en myndighet inte heller i en annan verksamhet än handläggning av ärenden kan ha full kontroll över vilka uppgifter som lämnas till myndigheten.

För att en viss behandling ska vara tillåten krävs också att behandlingen sker i enlighet med lagens övriga bestämmelser, exempelvis att de grundläggande kraven i 9 § PuL är uppfyllda (jfr 6 § första stycket 3).

11 § Personnummer eller samordningsnummer får tas in i ett beslut endast om beslutet rör en enskilds identitet eller motsvarande personliga förhållanden, det är nödvändigt för att beslutet ska kunna verk-

ställas eller det krävs med hänsyn till beslutande myndighets behov av identifieringsuppgifter.

I paragrafen regleras under vilka förutsättningar personnummer eller samordningsnummer får återges i ett beslut. Frågan behandlas i avsnitt 9.3.3.

I paragrafen anges uttömmande för vilka ändamål personnummer eller samordningsnummer får tas in i ett beslut. Det kan för det första vara frågan om att beslutet rör frågan om den registrerades identitet eller motsvarande personliga förhållanden – t.ex. namn eller civilstånd – exempelvis inom ramen för ett folkbokföringsärende. Något särskilt krav på att det är nödvändigt att personnumret eller samordningsnumret tas in i beslutet uppställs inte i det fallet. Ett personnummer eller samordningsnummer kan också behöva tas in i ett beslut för att beslutet ska kunna verkställas. I det fallet uppställs emellertid ett krav på nödvändighet. Det kan exempelvis handla om beslut som rör lagöverträdelser eller tvångsåtgärder av olika slag, beslut som i sig utgör en exekutionstitel mot den registrerade eller att personnumret eller samordningsnumret behöver återges eftersom den registrerades personuppgifter i övrigt är skyddade av sekretess. Det är också tillåtet att ta in ett personnummer eller samordningsnummer i ett beslut om det krävs med hänsyn till den beslutande myndighetens behov av identifieringsuppgifter. Så kan exempelvis vara fallet om en myndighet har byggt upp sin ärendehantering kring användning av personnummer eller samordningsnummer. Det kan då krävas att en sådan uppgift tas in i beslutet för att myndigheten ska kunna knyta det till rätt ärende.

Sökförbud

12 § Uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening liksom uppgifter som rör hälsa eller sexualliv får användas som sökbegrepp endast om det är tillåtet enligt föreskrifter som tagits in i bilaga till denna lag eller i annan lag eller förordning.

Vad som sägs i första stycket gäller inte vid en sökning i en viss handling eller i ett visst ärende.

I paragrafen anges under vilka förutsättningar sökbegrepp får användas som avslöjar känsliga personuppgifter. Frågan behandlas i avsnitt 9.4.2.

Enligt *första stycket* får uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening liksom uppgifter som rör hälsa eller sexualliv användas som sökbegrepp endast om det har tillåtits enligt särskild föreskrift i lag eller förordning. Bestämmelsen är alltså tillämplig på sökbegrepp som avslöjar eller rör känsliga personuppgifter i den mening som avses i 13 § PuL. Som huvudregel gäller därmed ett förbud för alla myndigheter som behandlar personuppgifter enligt lagen mot att använda sökbegrepp som avslöjar eller rör sådana uppgifter. Förbudet är av ett sådant absolut slag som innebär att myndigheten som sådan saknar befogenhet att göra en sammanställning. Den s.k. begränsningsregeln i 2 kap. 3 § tredje stycket TF är därmed tillämplig. Det innebär att myndigheten saknar befogenhet att göra en sammanställning som innehåller personuppgifter genom att använda ett sökbegrepp som avslöjar eller rör känsliga personuppgifter både för den egna verksamheten och för att uppfylla en begäran om en sådan sammanställning med stöd av 2 kap. 3 § andra stycket TF. Bestämmelsen är enbart tillämplig på en sökning som sker i syfte att göra en sammanställning som innehåller personuppgifter. Den tar alltså sikte på sammanställningar som görs av uppgifter som finns i en informationssamling där personuppgifter behandlas, exempelvis i en myndighets ärendehanteringssystem eller i ett visst register. Det sökbegrepp som används för att göra en sådan sammanställning behöver emellertid inte i sig utgöra en personuppgift. För att bestämmelsen ska vara tillämplig på ett visst sökbegrepp krävs dock att ett användande av begreppet leder till att känsliga personuppgifter sammanställs. Som exempel kan nämnas att ordet ”utmattningssyndrom” används som sökbegrepp för att sammanställa uppgifter om personer som har ansökt om sjukpenning.

Bestämmelsen är däremot inte tillämplig om motsvarande sökbegrepp används för att sammanställa uppgifter om vetenskaplig litteratur ur en referensdatabas. Den omständigheten att det i en sådan referensdatabas visserligen kan förekomma enstaka personuppgifter, exempelvis beträffande de författare som ingår där, innebär inte att det blir fråga om en sådan sökning som avses i bestämmelsen. En

sådan sökning torde över huvud taget inte vara att anse som en behandling av personuppgifter, dvs. det är ingen åtgärd som vidtas i fråga om personuppgifter (jfr 3 § PuL). Om det visar sig att sammanställningen innehåller personuppgifter när den väl är gjord kan det däremot bli aktuellt att beakta regler om personuppgiftsbehandling för sammanställningens fortsatta användning.

Genom *andra stycket* klargörs att bestämmelsen endast tar sikte på den situationen att en sökning görs för att sammanställa personuppgifter ur myndighetens informationssamlingar och inte då en sökning görs i en viss handling eller i ett visst ärende.

Elektroniskt utlämnande

Direktåtkomst

13 § Direktåtkomst till personuppgifter som är sekretessreglerade är tillåten endast i den utsträckning som anges i bilaga till denna lag eller i annan lag eller förordning. Med sekretessreglerade uppgifter avses detsamma som i offentlighets- och sekretesslagen (2009:400).

Vad som sägs i första stycket gäller inte direktåtkomst som medges

1. den registrerade eller dennes ombud till uppgifter som hänför sig till den registrerade,

2. till personuppgifter som är sekretessreglerade enligt 21 kap. 7 § offentlighets- och sekretesslagen,

3. ett personuppgiftsbiträde eller

4. en myndighet endast för sådan teknisk bearbetning eller teknisk lagring som avses i 2 kap. 10 § första stycket tryckfrihetsförordningen för den utlämnande myndighetens räkning.

I paragrafen anges under vilka förutsättningar direktåtkomst till personuppgifter som är sekretessreglerade får medges. Frågan behandlas i avsnitt 11.1.1 och 11.1.2.

Enligt *första stycket* gäller som huvudregel att en myndighet inte får medge direktåtkomst till sekretessreglerade personuppgifter om det inte finns stöd för det i lag eller förordning. Med sekretessreglerad uppgift avses detsamma som i offentlighets- och sekretesslagen, dvs. en uppgift för vilken det finns en bestämmelse om sekretess (jfr 3 kap. 1 § OSL). Med direktåtkomst avses att en myndighet har medgetts en sådan teknisk tillgång till upptagningar hos en annan

myndighet som avses i 2 kap. 3 § andra stycket TF, dvs. att upptagningen är tillgänglig med tekniska hjälpmedel som den mottagande myndigheten själv utnyttjar för överföring i sådan form att den kan läsas, avlyssnas eller på annat sätt uppfattas (jfr prop. 2007/08:160 s. 164). Om de upptagningar som en myndighet på detta sätt får tillgång till innehåller sekretessreglerade personuppgifter är alltså bestämmelsen tillämplig. Om en enskild aktör har medgetts en motsvarande åtkomst till sekretessreglerade personuppgifter hos en myndighet är den också att anse som direktåtkomst i paragrafens mening. Frågan om en myndighet ska eller får medge en enskild eller en annan myndighet direktåtkomst avgörs av hur stödet för en sådan åtgärd har formulerats i den aktuella lagen eller förordningen. Om det föreskrivs att en direktåtkomst får medges, vilket hittills har varit den vanligaste formen av författningsstöd, är det den myndighet som avses lämna ut uppgifter genom direktåtkomst som avgör om direktåtkomsten ska medges också i praktiken. I ett sådant fall ankommer det alltså på den utlämnande myndigheten att avgöra om direktåtkomsten faktiskt ska komma till stånd. Den bedömningen får göras med utgångspunkt i tillämpligt författningsstöd för den aktuella direktåtkomsten samt med beaktande av vad som gäller för uppgiftsutbytet i bestämmelser om sekretess och i andra föreskrifter, exempelvis i denna lag om behandling av personuppgifter.

I *andra stycket* anges att vissa undantag gäller från kravet på stöd i lag eller förordning.

Enligt *punkten 1* krävs inte stöd i lag eller förordning för att medge den registrerade eller dennes ombud direktåtkomst till sekretessreglerade uppgifter som hänför sig till den registrerade själv. Det ska alltså vara frågan om personuppgifter som kan knytas till den registrerade i den mening som avses i 3 § PuL. För att ett ombud ska kunna medges direktåtkomst utan stöd i lag eller förordning förutsätts att det är fråga om uppgifter för vilka den registrerade själv kan efterge sekretessen enligt 12 kap. 2 § OSL och att det finns ett behov av de uppgifter som kan lämnas ut genom direktåtkomsten för den angelägenhet som ombudets behörighet avser. Ett samtycke från den registrerade till att hans eller hennes ombud kan medges direktåtkomst till sekretessreglerade uppgifter kan enbart ta sikte på frågan om uppgifterna kan lämnas ut utan hinder av sekretess. Frågan om på vilket sätt uppgifterna ska lämnas ut, dvs. genom direktåtkomst eller på annat sätt, ankommer på den utläm-

nande myndigheten att avgöra. Den registrerade har ju exempelvis inte möjlighet att avgöra om direktåtkomst kan medges med hänsyn till de krav på informationssäkerhet som gäller för myndigheten.

I *punkten 2* anges att kravet på stöd i lag eller förordning inte heller gäller direktåtkomst till personuppgifter som är sekretessreglerade enligt 21 kap. 7 § OSL, dvs. den s.k. PuL-sekretessen.

Genom *punkten 3* klargörs att kravet på stöd i lag eller förordning för att få medge direktåtkomst till personuppgifter som är sekretessreglerade inte heller gäller om en sådan åtkomst medges ett personuppgiftsbiträde. Med personuppgiftsbiträde avses detsamma som i personuppgiftslagen, dvs. den som behandlar personuppgifter för den personuppgiftsansvariges räkning (jfr 3 § PuL). Ett personuppgiftsbiträde får bara behandla personuppgifter i enlighet med instruktioner från den personuppgiftsansvariga myndigheten. För att direktåtkomst ska kunna medges ett personuppgiftsbiträde utan stöd i lag eller förordning förutsätts därför att det finns ett sådant avtal om personuppgiftsbiträdets behandling som avses i 21 § denna lag som bl.a. innehåller sådana instruktioner.

Enligt *punkten 4* behövs inte heller något stöd i lag eller förordning för att medge en annan myndighet direktåtkomst till sekretessreglerade uppgifter, om den myndigheten förvarar uppgifterna enbart som ett led i en sådan teknisk bearbetning eller en teknisk lagring som avses i 2 kap. 10 § första stycket TF för den utlämnande myndighetens räkning. Enligt det lagrummet anses inte heller de handlingar i vilka uppgifterna ingår som allmänna hos den mottagande myndigheten. Om den mottagande myndigheten emellertid avser att använda de personuppgifter som blir åtkomliga genom direktåtkomsten för något annat syfte än de som anges i 2 kap. 10 § TF, är undantaget från kravet på författningsstöd inte tillämpligt.

14 § Innan en myndighet medger direktåtkomst till personuppgifter ska myndigheten göra en risk- och sårbarhetsanalys och komma överens med mottagaren av personuppgifterna hur skyddet för personuppgifterna ska säkerställas. Av överenskommelsen ska också framgå hur utövandet av de skyldigheter som personuppgiftsansvaret innefattar ska ske.

Vad som sägs i första stycket ska i tillämpliga delar även gälla då en myndighet på annat sätt än genom direktåtkomst samarbetar med andra

myndigheter eller enskilda på sätt som innebär behandling av personuppgifter i gemensamma eller annars integrerade informationssystem.

Paragrafen anger krav på att personuppgiftsansvarig myndighet vidtar vissa förberedande åtgärder i samband med direktåtkomst och liknande samverkan i integrerade informationssystem. Frågan behandlas i avsnitt 10.1.4 och 10.2.5.

Enligt *första stycket* gäller ett krav på en personuppgiftsansvarig myndighet att innan direktåtkomst medges till personuppgifter som myndigheten ansvarar för dels göra en risk- och sårbarhetsanalys, dels komma överens med mottagaren angående hur personuppgifterna ska skyddas genom tekniska och organisatoriska säkerhetsåtgärder och om hur inblandade aktörer avser fördela utövandet av de skyldigheter som personuppgiftsansvaret innefattar. Hur personuppgiftsansvaret är fördelat vid direktåtkomst följer av 7 § andra stycket denna lag. Bestämmelsen omfattar direktåtkomst oavsett om den är författningsreglerad eller inte, dvs. den gäller även vid direktåtkomst till personuppgifter som inte är sekretessreglerade. Den särskilda risk- och sårbarhetsanalys som ska göras avseende den planerade direktåtkomsten ska inriktas på att ge det underlag som behövs för att sedan kunna bedöma vilka tekniska och organisatoriska säkerhetsåtgärder som måste vidtas för att i enlighet med lagens krav åstadkomma en lämplig säkerhetsnivå till skydd för personuppgifterna. Vidare måste en överenskommelse göras på förhand där den utlämnande myndigheten och mottagaren eller mottagarna reder ut och klargör mellan sig hur skyddet för personuppgifterna ska säkerställas genom tekniska och organisatoriska säkerhetsåtgärder. I kravet på överenskommelse ligger också att de inblandade myndigheterna eller enskilda aktörerna reder ut hur personuppgiftsansvaret är tänkt att utövas, t.ex. om den praktiska hanteringen av ansvaret eventuellt ska fördelas mellan de ingående aktörerna. Personuppgiftsansvaret som sådant kan dock aldrig regleras genom överenskommelsen. Överenskommelsens syfte är enbart att utövandet av personuppgiftsansvarets olika moment ska klarläggas och arbetsuppgifter eventuellt fördelas mellan aktörerna. Överenskommelsen ska omfatta såväl säkerhetsåtgärder som andra skyldigheter som följer med personuppgiftsansvaret. Det förstnämnda kan t.ex. handla om frågor såsom vem som ska ansvara för olika funktioner, säkerhetslösningar, loggning och kontroller. Det sistnämnda kan t.ex. omfatta utarbetandet

av gemensamma rutiner som underlättar för registrerade att utnyttja sina rättigheter i fråga om korrigering eller information. Rutiner för samarbete mellan involverade personuppgiftsombud eller utseende av ett gemensamt ombud då det är frågan om komplexa system för informationsutbyte m.m. kan vara en annan fråga som bör tas upp i överenskommelsen. Inget hindrar alltså att aktörerna genom överenskommelsen mellan sig fördelar det praktiska ombesörjandet av olika uppgifter så länge som en heltäckande efterlevnad av skyldigheterna enligt lagen uppnås. Ansvaret för att överenskommelser i dessa frågor träffas ligger på den utlämnande myndigheten. I personuppgiftsansvaret ingår att följa upp och kontrollera att överenskommelsen fungerar och följs i samarbetet.

Enligt *andra stycket* gäller motsvarande krav på risk- och sårbarhetsanalyser och överenskommelser när en myndighet genom andra former än direktåtkomst samarbetar på sätt som innefattar behandling av personuppgifter i gemensamma eller annars integrerade informationssystem, t.ex. genom förvaltningsgemensamma e-tjänster.

Annat utlämnande i elektronisk form

15 § Får en personuppgift lämnas ut till en enskild, kan det ske i elektronisk form om det inte är olämpligt med hänsyn till skyddet för personuppgiften.

I paragrafen erinras om att personuppgifter som får lämnas ut, kan lämnas ut till enskilda i elektronisk form om det inte är olämpligt. Frågan behandlas i avsnitten 11.2.2–11.2.4.

Paragrafens utgångspunkt är att personuppgifter som en myndighet får lämna ut, kan lämnas ut inte bara till andra myndigheter utan även till enskilda i elektronisk form. Med utlämnande i elektronisk form avses ett annat elektroniskt utlämnande än genom direktåtkomst. Det kan alltså vara frågan om att personuppgifter exempelvis lämnas ut genom ett usb-minne eller en cd-skiva eller att uppgifterna sänds över via e-post eller genom någon annan form av elektroniskt kommunikationsmedel. Att personuppgifter får lämnas ut innebär att det inte finns något hinder med hänsyn till sekretess mot att lämna ut uppgifterna eller att bestämmelser om behandling av personuppgifter inte hindrar ett utlämnande. Den senare bedöm-

ningen behöver göras om det är personuppgifter som lämnas ut utan att det har sin grund i att den enskilde begär ut handlingarna med stöd av rätten att ta del av allmänna handlingar enligt 2 kap. TF, exempelvis om myndigheten lämnar ut uppgifterna på eget initiativ eller som en serviceåtgärd. Enbart den omständigheten att den enskilde önskar att i elektronisk form få en allmän handling eller en sammanställning av uppgifter enligt 2 kap. 3 § andra stycket TF innebär emellertid inte att det är frågan om ett utlämnande som sker på annan grund än 2 kap. TF (jfr SOU 2010:4 s. 307). I bestämmelsen erinras alltså om att bedömningen av om det är olämpligt att lämna ut en personuppgift i elektronisk form ska göras först efter att myndigheten har tagit ställning till om personuppgiften – eller den handling i vilken den ingår – alls kan lämnas ut.

Utgångspunkten enligt paragrafen är att elektroniskt utlämnande ska kunna ske. I paragrafen erinras dock om att myndigheten inte bör lämna ut personuppgifter i elektronisk form om det är olämpligt. De lämplighetsaspekter som bestämmelsen tar sikte på avser enbart sådant som har samband med skyddet av personuppgifterna vid en sådan utlämnandeform. Det ska alltså vara aspekter som rör persondataskydd i samband med ett utlämnande av personuppgifter och som inte fångas upp av vare sig sekretessbestämmelser eller på ett uttryckligt sätt av den nya lagens bestämmelser om behandling av personuppgifter. Det skulle exempelvis kunna handla om att myndigheten inte förfogar över en teknik som innebär att uppgifterna kan förmedlas till mottagaren i elektronisk form på ett tillräckligt säkert sätt. Sådana aspekter som att myndigheten saknar resurser eller att elektroniskt utlämnande bedöms olämpligt med hänsyn till risk för minskade avgiftsintäkter utgör däremot inte sådana hinder mot att lämna ut personuppgifter i den mening som bestämmelsen avser att erinra om. Frågan om den typen av aspekter innebär att det är olämpligt att lämna ut uppgifter i elektronisk form får avgöras med utgångspunkt i exempelvis föreskrifter om myndigheters servicenivå. Som exempel på sådana föreskrifter kan nämnas förordningen (2003:234) om tiden för tillhandahållande av domar och beslut, m.m. som gäller för domstolar och statliga förvaltningsmyndigheter.

Överföring till tredjeland

16 § Utöver vad som följer av 34 § personuppgiftslagen (1998:204) eller av föreskrifter eller beslut som meddelats med stöd av 35 § samma lag får personuppgifter överföras till tredjeland som saknar adekvat skyddsnivå, om

1. överföringen krävs för handläggningen av ett visst ärende, eller

2. överföringen är nödvändig för att fullgöra en uppgiftsskyldighet som följer av lag eller förordning eller avtal med annan stat eller mellanfolklig organisation som Sverige har tillträtt eller annars är förpliktat att följa.

I paragrafen föreskrivs två undantag från förbudet att överföra personuppgifter till tredjeland som saknar adekvat skyddsnivå utöver de undantag som framgår genom hänvisningen i 6 § första stycket 7 till personuppgiftslagens överföringsbestämmelser. Frågan har behandlats i avsnitt 12.5.

Enligt *punkten 1* får personuppgifter överföras om det krävs för myndighetens handläggning av ett ärende. Så kan t.ex. vara fallet när en part i ärendet tillfälligt eller permanent befinner sig i tredjeland. Undantaget är bara tillämpligt om överföringen krävs i det särskilda fallet, dvs. för handläggningen av ett visst ärende. Det innebär att myndigheten vid kommunikation i samband med en viss ärendehandläggning inte behöver göra en bedömning av om skyddsnivån i mottagarlandet är adekvat eller inte (33 § PuL). Den bedömning som i stället ska göras är om överföringen krävs för handläggningen av ärendet eller inte. Det är dock viktigt att myndigheten vid överföring även beaktar frågan om någon särskild säkerhetsåtgärd kan och bör vidtas för att skydda uppgifterna. Myndigheten kan exempelvis behöva beakta om det förefaller olämpligt att översända uppgifterna i elektronisk form.

Enligt *punkten 2* får personuppgifter översändas till tredjeland, om en överföring av personuppgifter är nödvändig för att fullgöra en uppgiftsskyldighet som följer av lag eller förordning eller ett för Sverige bindande internationellt avtal. Även vid överföring enligt denna punkt måste överföringen ske med godtagbar säkerhet till skydd för uppgifterna.

Säkerhet vid behandlingen

17 § En myndighet ska vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder för att skydda de personuppgifter som behandlas. Säkerhetsarbetet ska omfatta förebyggande, löpande och uppföljande åtgärder samt åstadkomma en lämplig säkerhetsnivå i förhållande till de risker som behandlingen medför och karaktären hos de uppgifter som ska skyddas. Vid utformningen av säkerhetsåtgärderna ska myndigheten även beakta bestämmelser om informationssäkerhet i annan författning som gäller för myndigheten.

I paragrafen regleras personuppgiftsansvariga myndigheters skyldighet att skydda personuppgifter med lämpliga säkerhetsåtgärder. Frågan behandlas i avsnitt 10.2.5.

Enligt paragrafen ska personuppgiftsansvariga myndigheter vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder för att skydda de personuppgifter som behandlas samt åstadkomma en lämplig säkerhetsnivå i förhållande till de risker som behandlingen medför och karaktären hos de uppgifter som ska skyddas. Bestämmelsen motsvarar i princip 31 § första stycket PuL. En skillnad är emellertid tydliggörandet av att säkerhetsarbetet ska ske systematiskt och omfatta samtliga led i personuppgiftsbehandlingen, dvs. arbetet ska inbegripa förebyggande, löpande och uppföljande åtgärder. Vidare framgår av bestämmelsen att säkerhetsarbetet ska bedrivas så att det både inriktas på åtgärder som behövs för att skydda registrerades integritet och så långt möjligt samordnas med övrigt informationssäkerhetsarbete som sker i enlighet med t.ex. arkivlagstiftningen och andra föreskrifter om informationssäkerhet hos myndigheter.

18 § Tillgången till personuppgifter ska begränsas till vad varje anställd behöver för att kunna fullgöra sina arbetsuppgifter.

Paragrafen reglerar den interna tillgången till personuppgifter för myndighetens personal eller andra som deltar i myndighetens arbete. Frågan behandlas i avsnitt 10.2.5.

Paragrafen innebär en skyldighet för varje myndighet att se till att anställda bara ges tillgång till personuppgifter utifrån vad som krävs för arbetsuppgifterna. Bestämmelsen får anses även omfatta krav på behovsanpassning i fråga om andra som deltar i arbetet hos

myndigheten i egenskap av t.ex. praktikanter eller inhyrd bemanningspersonal. Krav på säkerhetsåtgärder i form av exempelvis behörighetsstyrning till elektroniska informationssamlingar syftar till att minska den interna exponeringen för personuppgifterna. Hur detta ska ske får bedömas utifrån en analys av förutsättningarna och behoven inom varje myndighet. Faktorer som myndighetens och informationssystemens storlek samt huruvida personuppgifterna är sekretessreglerade eller annars integritetskänsliga är härvid centrala. Bestämmelsen omfattar inte bara tillgången till myndighetens egen information. Vid direktåtkomst är det den mottagande myndigheten som ansvarar för att se till att den egna personalen inte ges en vidare tillgång till åtkomliga uppgifter hos den utlämnande myndigheten än vad arbetsuppgifterna motiverar. Det är en annan sak att behörighetsbegränsningar rent tekniskt kan anordnas hos den av myndigheterna där det är enklast. Frågor av dessa slag bör redas ut mellan involverade myndigheter innan en direktåtkomst faktiskt etableras, se 14 § om överenskommelse vid direktåtkomst.

Personuppgiftsbiträde

19 § Ett personuppgiftsbiträde eller den som arbetar under biträdets ledning får behandla personuppgifter bara i enlighet med instruktioner från den personuppgiftsansvariga myndigheten. Detta gäller även för biträden som anlitats av ett personuppgiftsbiträde.

Paragrafen reglerar vad som gäller för behandlingen av personuppgifter hos personuppgiftsbiträdet. Frågan behandlas i avsnitt 10.1.4.

Bestämmelsen motsvarar 30 § första stycket PuL. Det klargörs dock att samma begränsningar även gäller för s.k. underbiträden och personal hos denne, dvs. sådana personuppgiftsbiträden som med den personuppgiftsansvariga myndighetens samtycke anlitas av ett personuppgiftsbiträde, se 20 § 4.

20 § När en myndighet anlitar ett personuppgiftsbiträde, ska myndigheten förvissa sig om att biträdet

1. ser till att personuppgifter behandlas bara i enlighet med instruktioner från myndigheten,

2. kan genomföra de säkerhetsåtgärder som avses i 17 § och som måste vidtas till skydd för de personuppgifter som biträdet behandlar,

3. fortlöpande vidtar säkerhetsåtgärderna, och

4. inte anlitar annat biträde utan godkännande från myndigheten.

I paragrafen ställs vissa minimikrav på vad den personuppgiftsansvariga myndigheten måste förvissa sig om vid anlitande av ett personuppgiftsbiträde. Frågan behandlas i avsnitt 10.1.4.

Paragrafen motsvarar i princip vad som följer av 31 § andra stycket PuL men förskriver några ytterligare förutsättningar som den personuppgiftsansvariga myndigheten måste förvissa sig om är uppfyllda innan ett personuppgiftsbiträde anlitas. Myndigheten ska se till att personuppgifter behandlas hos personuppgiftsbiträdet bara i enlighet med instruktioner från myndigheten (punkten 1), att personuppgiftsbiträdet kan genomföra de säkerhetsåtgärder som avses i 17 § och som måste vidtas till skydd för de personuppgifter som biträdet behandlar (punkten 2) och att biträdet fortlöpande vidtar säkerhetsåtgärderna (punkten 3). Genom dessa punkter framgår bl.a. att myndighetens kontroll måste vara uppföljande. Vidare är myndigheten skyldig att se till att personuppgiftsbiträdet inte i sin tur anlitar ett personuppgiftsbiträde, ett underbiträde, för att sköta viss del av personuppgiftsbehandlingen, utan att det har föregåtts av ett särskilt godkännande från den personuppgiftsansvariga myndigheten (punkten 4).

21 § Det ska finnas ett skriftligt avtal om personuppgiftsbiträdets behandling av personuppgifter för myndighetens räkning. Avtalet ska innehålla instruktioner och villkor om personuppgiftsbiträdets skyldigheter i frågor som avses i 19 och 20 §§. Motsvarande avtal ska finnas med ett biträde som anlitats av ett personuppgiftsbiträde.

I paragrafen regleras personuppgiftsbiträdesavtalet till form och innehåll. Frågan behandlas i avsnitt 10.1.4.

Liksom motsvarande bestämmelse i 30 § andra stycket PuL uppställs i paragrafen ett krav på att avtal med ett personuppgiftsbiträde ska ha skriftlig form. Vidare anges i paragrafen vad avtalet ska innehålla, nämligen instruktioner och föreskrivna villkor om personuppgiftsbiträdets skyldigheter i frågor som avses i 19 och 20 §§. Avtalet ska således innehålla villkor om att personuppgifts-

biträdet eller den som arbetar under biträdets ledning får behandla personuppgifter bara i enlighet med instruktioner från den personuppgiftsansvariga myndigheten. Vidare ska avtalet innehålla en dokumentation av dels myndighetens instruktioner till biträdet, dels villkor om säkerhetsåtgärder som biträdet måste vidta. Instruktionerna och villkoren kan avse en mängd olika slags frågor, exempelvis för vilket ändamål personuppgifter får behandlas, hur tillgången till uppgifterna ska begränsas eller andra säkerhetsåtgärder, hur registrerades rättigheter till information m.m. ska tillgodoses, vad som ska hända med uppgifterna när uppdraget slutförts och rutiner för hur den personuppgiftsansvariga myndigheten ska kunna kontrollera behandlingen hos biträdet m.m. Avtalet ska också innehålla villkor om att biträdet inte anlitar ett underbiträde utan den personuppgiftsansvariga myndighetens godkännande. För det fall ett underbiträde anlitas, ska ett motsvarande avtal tecknas med denne.

Förteckning över behandlingar

22 § En myndighet ska föra en förteckning över de behandlingar som myndigheten utför med stöd av denna lag.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela närmare föreskrifter om vilka uppgifter en sådan förteckning ska innehålla.

I paragrafen regleras en skyldighet att föra en förteckning över personuppgiftsbehandlingar. Frågan behandlas i avsnitt 16.4.1.

Enligt *första stycket* ska en personuppgiftsansvarig myndighet vara skyldig att föra en förteckning över de personuppgiftsbehandlingar som myndigheten utför med stöd av lagen. Syftet med förteckningen är att registrerade och allmänhet på ett enkelt sätt, genom att få del av den allmänna handling som förteckningen utgör, ska kunna få övergripande information om den behandling av personuppgifter som myndigheten utför, dvs. såväl sådan som faktiskt sker inom myndigheten som sådan som sker hos ett personuppgiftsbiträde. I uttrycket ”föra en förteckning” innefattas att förteckningen ska uppdateras regelbundet så att den avspeglar aktuella förhållanden. I praktiken torde arbetet med förteckningen kunna samordnas med

arbetet att ta fram beskrivningar av myndighetens allmänna handlingar och arkiv.

I *andra stycket* upplyses om att regeringen eller den myndighet regeringen bestämmer meddelar närmare föreskrifter om förteckningens innehåll. Utgångspunkten är att innehållet i förteckningen i vart fall ska motsvara vad en anmälan till tillsynsmyndigheten skulle ha innehållit enligt artikel 19.1 a–e dataskyddsdirektivet (jfr 36 § PuL och anknytande föreskrifter).

Undantag från informationsskyldigheten

23 § Bestämmelserna i 23, 25 och 26 §§ personuppgiftslagen (1998:204) ska inte tillämpas i den utsträckning som en uppgift inte får lämnas ut till den registrerade på grund av sekretess enligt offentlighets- och sekretesslagen (2009:400) eller föreskrifter som meddelats med stöd av den lagen.

Bestämmelserna i 26 § personuppgiftslagen behöver inte tillämpas vid behandling av personuppgifter som inte ingår i eller är avsedda att ingå i en samling av personuppgifter som har strukturerats för att påtagligt underlätta sökning efter eller sammanställning av personuppgifter.

I paragrafen anges vissa undantag från skyldigheten att informera registrerade om behandlingar rörande denne. Frågorna har behandlats i avsnitt 13.4.2 och 13.4.3.

Enligt *första stycket* gäller inte skyldigheten enligt 6 § första stycket 5 och 6 att lämna information som avses i 23, 25 och 26 §§ PuL i den mån sekretess för uppgifter gäller i förhållande till den registrerade. Så kan vara fallet för uppgift som omfattas av sekretess till skydd för ett allmänt intresse eller till skydd för någon annan enskilds intresse. Bestämmelsen motsvarar 27 § PuL.

I *andra stycket* undantas personuppgifter i s.k. ostrukturerat material från skyldigheten att lämna information efter ansökan enligt 26 § PuL. Bestämmelsen motsvarar i detta avseende missbruksregeln i 5 a § första stycket PuL. För närmare ledning angående vad som avses med personuppgifter som inte ingår i eller är avsedda att ingå i en samling av personuppgifter som har strukturerats för att påtagligt underlätta sökning efter eller sammanställning av personuppgifter hänvisas till förarbetena till 5 a § PuL (prop. 2005/06:173

s. 19 f. och s. 58, se även Öman/Lindblom, s. 131 f.). Undantaget har den praktiska betydelsen att myndigheter inte behöver använda tillgängliga sök- eller sammanställningsfunktioner i fråga om ostrukturerat material, t.ex. i e-postsystem, anställdas hårddiskar m.m. när information begärs.

Korrigering av felaktiga personuppgifter eller annars otillåten behandling

24 § En personuppgift ska på begäran av den registrerade rättas eller kompletteras om uppgiften rör honom eller henne och den är felaktig eller ofullständig till följd av en åtgärd som inte har sin grund i myndighetens eller någon annans bedömning.

I paragrafen anges i vilken utsträckning myndigheten är skyldig att på begäran av den registrerade rätta eller komplettera en personuppgift som är felaktig eller ofullständig till följd av en åtgärd som inte har sin grund i en bedömning som har gjorts av myndigheten eller av någon annan, som har försett myndigheten med personuppgiften. Frågan behandlas i avsnitt 15.4.1–15.4.3.

Genom bestämmelsen ges den registrerade en rätt att begära att en myndighet ska vidta åtgärder för att rätta eller komplettera en personuppgift som den registrerade anser bör rättas eller kompletteras. Av bestämmelsen följer en skyldighet för en myndighet att rätta eller komplettera en personuppgift som är felaktig eller ofullständig. En sådan skyldighet finns om felaktigheten eller ofullständigheten har sin grund i en åtgärd som inte beror på myndighetens eller någon annans bedömning. Det kan exempelvis vara frågan om sådana förbiseendefel som avses i 26 § FL eller ett fel som uppstått p.g.a. något tekniskt förfarande. Den registrerade har däremot inte rätt att begära en rättelse enligt denna bestämmelse i det fall han eller hon anser att personuppgiften inte är relevant eller för gammal med hänsyn till det ändamål för vilket behandlingen äger rum. En begäran om korrigering i ett sådant fall får i stället bedömas med tillämpning av den bestämmelse som finns i 25 §, se kommentaren till den paragrafen. Den registrerades rätt att begära att en personuppgift ska rättas eller kompletteras och myndighetens skyldighet att vidta åtgärder om uppgiften visar sig vara felaktig eller ofullständig i objektiv mening gäller oavsett i vilket sammanhang person-

uppgiften behandlas. Bestämmelsen är alltså tillämplig både på personuppgifter som tagits in i en myndighets beslut och i andra dokument eller uppgiftssamlingar, exempelvis ett register.

25 § En personuppgift ska på begäran av den registrerade avskiljas från fortsatt behandling och inte lämnas ut till en enskild annat än med stöd av 2 kap. tryckfrihetsförordningen eller utplånas, om uppgiften rör honom eller henne och den inte får behandlas enligt denna lag.

Vad som sägs i första stycket gäller inte personuppgifter i ett beslut.

I paragrafen anges under vilka förutsättningar en myndighet på begäran av en registrerad ska korrigera en behandling som inte uppfyller lagens krav. Frågan behandlas i avsnitten 15.4.1, 15.4.2 och 15.4.4.

Enligt *första stycket* är en myndighet skyldig att på begäran av den registrerade korrigera en behandling av personuppgifter som rör honom eller henne och som inte uppfyller lagens krav. Av de grundläggande kraven i 9 § PuL följer en allmän skyldighet för den personuppgiftsansvarige att se till att personuppgifter bara behandlas om det är lagligt och att det alltid sker på ett korrekt sätt. Genom paragrafen görs klart att en myndighet är skyldig att agera om en registrerad påpekar att en behandling av personuppgifter som rör honom eller henne inte uppfyller lagens krav. För att det ska vara fråga om en skyldighet som följer av paragrafen ska det gälla påpekanden som tar sikte på att en behandling av personuppgifter brister i något annat avseende än de som avses i 24 §, dvs. i något annat avseende än att uppgifterna är i objektiv mening oriktiga eller ofullständiga. Det ska vara fråga om påpekanden som kan bekräftas överensstämma med de krav som gäller för den aktuella behandlingen först efter en bedömning från myndighetens sida och som inte kan åtgärdas genom att personuppgifterna rättas eller kompletteras. Det ska alltså vara fråga om påpekanden från den registrerade som rör att behandlingen av de aktuella personuppgifterna i något avseende inte alls är tillåten. Som exempel kan nämnas att den registrerade gör gällande att uppgifterna har behandlats under för lång tid och därför inte får behandlas längre, att stöd saknas för att behandla uppgifter eftersom de utgör känsliga personuppgifter eller att uppgifterna inte kan anses relevanta för det ändamål för vilket behandlingen äger rum.

Om det bedöms att behandlingen inte uppfyller de krav som gäller för den följer av bestämmelsen att myndigheten är skyldig att vidta åtgärder. De åtgärder som omnämns i paragrafen är avskiljande eller utplåning av personuppgifter. Begreppet avskiljande syftar till att ersätta termen blockering som används i personuppgiftslagen. Av paragrafen följer, i likhet med vad som är fallet enligt 28 § PuL, att det i princip står myndigheten fritt att välja vilken åtgärd som ska vidtas. För myndigheternas del är detta en princip som emellertid är förenad med betydande undantag när det gäller personuppgifter som ingår i handlingar som är allmänna enligt 2 kap. TF. Grundlagsbestämmelserna i 2 kap. TF gäller före den nya lagen. Detsamma gäller bestämmelser om arkivering av allmänna handlingar (jfr 8 § andra stycket PuL). Om en myndighet konstaterar att en personuppgift som ingår i en allmän handling har behandlats längre än vad som är tillåtet enligt en gallringsföreskrift, ska den allmänna handlingen eller en del av den gallras enligt den föreskriften. Den nya lagen innehåller således inte några egna bestämmelser om gallring. Åtgärden gallring omfattas därför inte av den nu aktuella paragrafen.

En korrigeringsåtgärd som anvisas i paragrafen och som myndigheten i normalfallet kan vidta för att korrigera en behandling som inte är tillåten är att avskilja de aktuella personuppgifterna från en fortsatt behandling. Att en uppgift avskiljs, exempelvis för att den inte är relevant för det aktuella ändamålet, innebär att den tas bort från den behandling där den inte längre ska förekomma. Som exempel kan nämnas att det bedömts att det inte är relevant att den aktuella myndigheten behandlar personuppgiften i fråga genom att offentliggöra den på myndighetens webbplats med hänsyn till det ändamål för vilket publiceringen sker. Om personuppgiften tas bort från informationen på webbplatsen genom att informationen som finns där anonymiseras, innebär det att personuppgiften har avskilts från den behandling som sker på webbplatsen. Personuppgiften kan därefter behandlas på något annat sätt och för något annat ändamål som då är berättigat, exempelvis att den allmänna handling där personuppgiften ingår tillhandahålls på ett annat sätt eller att handlingen arkiveras. Om en registrerad anser att en personuppgift som rör honom eller henne har behandlats för länge med hänsyn till vad som sägs i en tillämplig gallringsföreskrift, har den registrerade alltså inte rätt att med stöd av den nu aktuella bestämmelsen begära att den allmänna handlingen där personuppgiften ingår helt eller delvis

gallras. Däremot har den registrerade rätt att begära att uppgiften avskiljs. Det ankommer därefter på myndigheten att bedöma om så ska ske, och om uppgiften eventuellt också ska gallras. Den senare åtgärden sker emellertid då med stöd av en tillämplig gallringsföreskrift och inte på grund av vad som sägs i denna lag.

Av paragrafen följer att en otillåten behandling också kan åtgärdas genom att personuppgifter utplånas. Med utplåning avses samma slags åtgärd som i 28 § PuL. Att utplåna en personuppgift innebär att det automatiserade medium där de aktuella personuppgifterna behandlas förstörs eller att uppgifterna i mediet förstörs så att informationen om personuppgifterna inte kan återskapas (jfr Öman/Lindblom, s. 418 f.). Med arkivlagstiftningens terminologi torde utplånande av en personuppgift i en allmän handling närmast avse gallring genom förstöring av handlingen i fråga eller att uppgifterna i handlingen förstörs (se 2 kap. 1 § Riksarkivets föreskrifter RA-FS 2009:1). För att en allmän handling ska gallras genom att den förstörs eller uppgifter i den förstörs krävs att det finns stöd för det i en gallringsföreskrift. Stöd för att i andra fall förstöra en allmän handling eller uppgifter i en allmän handling finns endast i undantagsfall, exempelvis i fråga om patientjournaler som kan förstöras efter ansökan till Socialstyrelsen (jfr 8 kap. 4 § patientdatalagen [2008:355]). Saknas ett sådant särskilt författningsstöd eller stöd i en gallringsföreskrift torde en myndighet alltså inte kunna utplåna personuppgifter i en allmän handling på begäran av den registrerade. Utrymmet för en myndighet att på begäran av en registrerad utplåna personuppgifter enbart med stöd av den nu aktuella bestämmelsen torde därför vara begränsat och kan alltså endast avse personuppgifter i handlingar som inte är allmänna.

Tillsynsmyndighetens befogenheter

26 § Tillsynsmyndigheten har rätt att för sin tillsyn på begäran få

1. tillgång till de personuppgifter som behandlas,

2. upplysningar om och dokumentation av behandlingen av personuppgifter och säkerheten vid denna, och

3. tillträde till sådana lokaler som har anknytning till behandlingen av personuppgifter.

I paragrafen, som motsvarar 43 § PuL, anges vilka befogenheter tillsynsmyndigheter har för att undersöka om en myndighet behandlar personuppgifter på ett tillåtet sätt. Frågan behandlas i avsnitt 17.3.2.

27 § Om tillsynsmyndigheten konstaterar att en myndighet kan komma att behandla personuppgifter på ett olagligt sätt, ska tillsynsmyndigheten genom påpekanden eller andra åtgärder som inte är tvingande försöka åstadkomma att myndigheten uppfyller sina skyldigheter enligt denna lag eller föreskrifter som meddelats med stöd av den.

I paragrafen anges de åtgärder som tillsynsmyndigheten ska vidta för att förebygga att en myndighet behandlar personuppgifter på ett otillåtet sätt. Frågan behandlas i avsnitt 17.3.3.

Genom paragrafen tydliggörs att tillsynsmyndigheten ska använda sig av åtgärder som inte har en tvingande karaktär endast i de fall då åtgärderna syftar till att förebygga att en behandling ska bli otillåten. Det kan exempelvis ske genom att tillsynsmyndigheten uppmanar en myndighet att utforma sin personuppgiftsbehandling på ett visst sätt för att behandlingen inte ska riskera att bli otillåten. Om behandlingen däremot konstateras vara otillåten ska åtgärder med stöd av denna bestämmelse inte användas.

28 § Tillsynsmyndigheten får förelägga en myndighet att uppfylla sina skyldigheter, om myndigheten inte uppfyller de krav som följer av denna lag eller föreskrifter som meddelats med stöd av den.

Av föreläggandet ska framgå vad tillsynsmyndigheten anser är nödvändigt för att avhjälpa de påtalade bristerna.

I paragrafen anges under vilka förutsättningar som tillsynsmyndigheten får förelägga en myndighet att vidta åtgärder för att korrigera en behandling. Frågan behandlas i avsnitt 17.3.4.

I *första stycket* ges tillsynsmyndigheten befogenhet att förelägga en myndighet att fullgöra sina skyldigheter. Som förutsättning för att ett föreläggande ska få meddelas gäller att den myndighet som det riktar sig mot såsom personuppgiftsansvarig inte uppfyller de krav som följer av lagen eller anslutande föreskrifter. Därmed avses samtliga föreskrifter i lagen eller i förordning eller andra föreskrifter som meddelats med stöd av lagen.

Av *andra stycket* framgår att föreläggandet ska innehålla uppgift om vad tillsynsmyndigheten anser är nödvändigt för att avhjälpa de brister som konstaterats finnas i fråga om en viss behandling. Tillsynsmyndigheten ska alltså använda sig av ett föreläggande i de fall konstaterade brister kan korrigeras genom någon form av åtgärd som inte innebär att behandlingen som sådan behöver upphöra. Som exempel kan nämnas att det i ett register som förs för ett berättigat ändamål behandlas uppgifter rörande en viss eller några personer som inte kan anses relevanta för ändamålet. En korrigering kan då ske genom att just dessa personuppgifter avskiljs från den behandling som sker i registret.

29 § Om en myndighet allvarligt brister i sin skyldighet att uppfylla de krav som gäller för en behandling av personuppgifter som myndigheten utför, får tillsynsmyndigheten förbjuda myndigheten att fortsätta behandlingen på något annat sätt än att personuppgifter lagras. Ett beslut om förbud mot fortsatt behandling gäller omedelbart.

I paragrafen anges under vilka förutsättningar som tillsynsmyndigheten får förbjuda en behandling. Frågan behandlas i avsnitt 17.3.4.

Genom paragrafen ges tillsynsmyndigheten befogenhet att besluta att en myndighet inte får fortsätta med en viss behandling. För att ett sådant förbud ska få meddelas förutsätts att myndighet på ett allvarligt sätt brister i sina skyldigheter enligt de krav som gäller för behandlingen. Det ska alltså vara frågan om sådana brister i det skydd som ska finnas för personuppgifterna som omfattas av behandlingen som inte kan avhjälpas genom att vissa åtgärder vidtas utan att ett fullgott skydd endast kan uppnås genom att behandlingen som sådan upphör. Som exempel kan nämnas att en viss behandling av personuppgifter sker för ett ändamål som inte kan anses berättigat med hänsyn till det uppdrag som myndigheten har såsom det har kommit till uttryck i myndighetens instruktion och andra styrande dokument.

30 § Tillsynsmyndigheten får hos förvaltningsrätten inom vars domkrets tillsynsmyndigheten är belägen ansöka om att sådana personuppgifter som har behandlats på ett olagligt sätt ska utplånas.

I paragrafen anges under vilka förutsättningar tillsynsmyndigheten får ansöka hos en förvaltningsrätt om utplåning av personuppgifter. Frågan behandlas i avsnitt 17.3.6.

Paragrafen motsvarar 47 § första stycket PuL.

Bemyndiganden

31 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om

1. när behandling av personuppgifter är tillåten,

2. vilka krav som ställs på en personuppgiftsansvarig myndighet, och

3. att känsliga personuppgifter får behandlas om det behövs med hänsyn till ett viktigt allmänt intresse.

Regeringen får meddela föreskrifter om begränsningar av möjligheterna att använda andra sökbegrepp än de som avses i 12 §.

I paragrafen anges de bemyndiganden som behövs för att regeringen eller den myndighet som regeringen bestämmer ska kunna meddela bestämmelser som utgör en särreglering i förhållande till lagen. Frågan behandlas i avsnitt 18.2.2.

Överklaganden

32 § Tillsynsmyndighetens beslut enligt denna lag om annat än föreskrifter får överklagas till allmän förvaltningsdomstol.

Tillsynsmyndigheten får bestämma att dess beslut ska gälla även om det överklagas.

I paragrafen anges när tillsynsmyndighetens beslut får överklagas. Frågan behandlas i avsnitt 18.3.3.

33 § Beslut om rättelse eller komplettering enligt 24 §, om avskiljande eller utplåning enligt 25 § och om information enligt 26 § personuppgiftslagen (1998:204) får överklagas till allmän förvaltningsdomstol.

Första stycket gäller inte för beslut av regeringen, Högsta domstolen, Högsta förvaltningsdomstolen eller riksdagens ombudsmän.

I paragrafen anges i vilken utsträckning den registrerade får överklaga en personuppgiftsansvarig myndighets beslut som myndigheten har fattat med stöd av lagen. Frågan behandlas i avsnitt 18.3.3.

Bestämmelsen innebär att en rätt att överklaga finns i de fall myndigheten fattar beslut som direkt berör den enskilde. Sådana beslut kan överklagas till allmän förvaltningsdomstol. Någon rätt att överklaga beslut som fattats av de högsta statsorganen finns emellertid inte.

34 § Andra beslut enligt denna lag än sådana som avses i 32 § och 33 § första stycket får inte överklagas.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Enligt paragrafen gäller att inte några andra beslut får överklagas än de som avses i övriga bestämmelser om överklagande. Någon rätt att med stöd av förvaltningslagen överklaga beslut som en myndighet har fattats med stöd av lagen finns alltså inte. Frågan behandlas i avsnitt 18.3.3.

21.2 Förslaget till lag om ändring i offentlighets- och sekretesslagen (2009:400)

10 kap.

28 §

Sekretess hindrar inte att en uppgift lämnas till en annan myndighet, om uppgiftsskyldighet följer av lag eller förordning.

Sekretess hindrar inte heller att en uppgift lämnas till en annan myndighet genom direktåtkomst enligt vad som föreskrivs i lag eller förordning.

Ytterligare sekretessbrytande bestämmelser och bestämmelser om undantag från sekretess finns i anslutning till berörda sekretessbestämmelser i avdelning IV–VI.

I paragrafen har ett nytt andra stycke införts med en sekretessbrytande bestämmelse vid direktåtkomst. Frågan behandlas i avsnitt 11.1.3. och 11.1.4.

Den nya bestämmelsen i andra stycket innebär att en föreskrift i lag eller förordning genom vilken en myndighet får eller ska medges

direktåtkomst blir i sig sekretessbrytande. Om en sådan bestämmelse införs behöver det alltså inte därutöver införas en bestämmelse som ska ha en sekretessbrytande effekt, exempelvis i form av en bestämmelse om uppgiftsskyldighet. Med direktåtkomst avses sådan teknisk tillgång till upptagningar hos en annan myndighet som avses i 2 kap. 3 § TF (jfr prop. 2007/08:160 s. 164). Det innebär att upptagningarna ska vara tillgängliga med tekniska hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att de kan läsas, avlyssnas eller uppfattas på annat sätt.

För att en bestämmelse om direktåtkomst ska vara sekretessbrytande krävs att den anges i lag eller förordning. Därmed knyter denna bestämmelse an till 13 § i förslaget till en ny lag om myndigheters personuppgiftsbehandling med krav på stöd i lag eller förordning för att direktåtkomst till sekretessreglerade personuppgifter ska få medges. Med lag avses, i likhet med 8 kap. 1 § OSL, också EU-förordning. Bestämmelsen tar emellertid endast sikte på att bryta sekretess då direktåtkomst medges svenska myndigheter, vilket stämmer överens med vad som gäller enligt första stycket. I fråga om direktåtkomst som medges utländska myndigheter gäller i stället vad som föreskrivs i 8 kap. 3 §. Bestämmelsen gäller inte heller i fråga om direktåtkomst som medges enskilda. Genom bestämmelsen bryts sekretess inte bara då en myndighet medges direktåtkomst till personuppgifter utan också då åtkomsten avser andra sekretessbelagda uppgifter.

För att en föreskrift i lag eller förordning om direktåtkomst ska ha en sekretessbrytande effekt enligt denna bestämmelse krävs att den har en sådan konkretion att det framgår i fråga om vilka uppgifter som sekretessen bryts. Det krävs vidare att den medgivna direktåtkomsten omfattar samtliga uppgifter som åtkomsten avses gälla, eftersom alla dessa uppgifter lämnas ut till den mottagande myndigheten i den stund åtkomsten faktiskt etableras.

Särskilt yttrande

av experten Per Furberg

Jag delar utredningens bedömning att det bör införas en myndighetsdatalag. Det framstår vidare som angeläget att den föreslagna regleringen genomförs så snart det blir möjligt. Jag har emellertid en annan uppfattning än utredningen när det gäller frågan om direktåtkomst.

Utredningen har byggt sitt förslag på vad som ska anses vara förvarat och inkommet enligt 2 kap. TF hos myndighet. Denna gräns, som är delvis oklar, föreslås således vara avgörande för huruvida s.k. direktåtkomst ska anses föreligga. Det hade enligt min mening varit önskvärt att närmare få belyst vari skillnaden mellan olika former av elektroniska utlämnanden består och vilka verkningarna kan antas bli från persondataskyddssynpunkt.

Till detta kommer det förbud som utredningen föreslår mot direktåtkomst, till personuppgifter som är sekretessreglerade, i annan utsträckning än som anges i lag eller förordning. En ny elektronisk tjänst där s.k. direktåtkomst aktualiseras, som avser sekretessreglerade uppgifter, måste därmed föregås av ett lagstiftningsärende eller ett ärende om en förordningsändring. Att införa eller bibehålla tjänster som bygger på annat automatiserat elektroniskt utlämnande än direktåtkomst kan bli en utmaning med beaktande av den otydlighet som kan komma att finnas. Sannolikt styrs utvecklingen istället mot en allt mer omfattande direktåtkomst, med de konsekvenser för upprätthållandet av gränser mellan myndigheter som det kan föra med sig.

Enligt min mening hade utredningens konsekvensanalys därför bort innefatta en bedömning av de risker och kostnader som detta kan antas föra med sig för bl.a. utvecklingen av elektronisk förvaltning och möjligheterna att ge enskilda den service som de förväntar sig i elektronisk miljö.

Kommittédirektiv 2011:86

Integritet, effektivitet och öppenhet i en modern e-förvaltning

Beslut vid regeringssammanträde den 6 oktober 2011

Sammanfattning av uppdraget

En särskild utredare ska se över den s.k. registerlagstiftningen och vissa därmed sammanhängande frågor i syfte att skapa rättsliga förutsättningar för en mer effektiv e-förvaltning, där såväl den enskildes rätt till personlig integritet som allmänhetens berättigade anspråk på insyn i den offentliga verksamheten tillgodoses. Utredaren ska bl.a.

- överväga om definitionen av begreppet ”allmän handling” i tryckfrihetsförordningen (TF) är lämpligt utformad när det gäller sådana uppgifter som en myndighet har tillgång till genom s.k. direktåtkomst hos en annan myndighet eller genom liknande former av elektroniskt utlämnande och, om utredaren anser att definitionen bör ändras, lämna förslag till ändring av denna,
- överväga om det finns skäl att i registerförfattningar bibehålla åtskillnaden mellan olika former av elektroniskt utlämnande,
- göra en översiktlig inventering av registerförfattningarna och närmare analysera hur dessa fungerar inom tre olika verksamhetsområden,
- med beaktande av utvecklingen inom EU och Europarådet utarbeta en generell modell för reglering av registerfrågor och,

med modellen som mall, lämna konkreta förslag till registerförfattningar inom de tre verksamhetsområdena, och

- överväga vilka typer av allmänna handlingar inom de tre verksamhetsområdena som den eller de aktuella myndigheterna ska ha skyldighet att lämna ut elektroniskt och lämna de förslag som dessa överväganden föranleder.

Förslagen ska syfta till att regleringen i tryckfrihetsförordningen och offentlighets- och sekretesslagen (2009:400, OSL) samt registerregleringen tillsammans inom respektive område ska utgöra en tydligare och mer lättillämpad helhet.

De delar av uppdraget som avser frågan om definitionen av ”allmän handling” bör ändras respektive om det finns skäl att i registerförfattningarna även fortsättningsvis bibehålla åtskillnaden mellan olika former av elektroniskt utlämnande, ska redovisas i ett delbetänkande senast den 1 december 2012. I den förstnämnda delen ska utredaren samråda med en parlamentarisk referensgrupp. Regeringen kommer, efter att ha inhämtat synpunkter från utredaren, att i tilläggsdirektiv precisera inom vilka tre verksamhetsområden som utredaren ska lämna förslag till registerförfattningar. Uppdraget ska slutredovisas senast den 1 december 2014.

Bakgrund

I princip all framställning av information hos myndigheterna sker numera på elektronisk väg. Myndigheterna tar dessutom i allt större utsträckning emot information genom elektronisk kommunikation. Härtill kommer att handlingar till stor del även lagras elektroniskt. När myndigheter ska utbyta uppgifter är det därför i stor utsträckning önskvärt att uppgiftslämnandet sker med hjälp av modern informationsteknik. Utökad elektronisk informationsöverföring mellan myndigheter effektiviserar beslutsprocesserna och medför fördelar för enskilda, eftersom insamlandet av korrekta och aktuella uppgifter underlättas och snabbare besked kan ges. Elektronisk informationsöverföring är också ekonomiskt effektiv i förhållande till uppgiftslämnande på annat sätt, t.ex. per telefon eller fax. Samtidigt är det av central betydelse att integritetsaspekterna beaktas.

Regeringen bedriver ett omfattande förvaltningspolitiskt reformarbete som bl.a. syftar till att effektivisera förvaltningen och förenkla mötet med medborgare och företag genom elektronisk förvaltning (prop. 2009/10:175 s. 25). I januari 2008 fastställde regeringen en handlingsplan för elektronisk förvaltning (Fi2008/491). I handlingsplanen anges som övergripande mål för e-förvaltningen att det ska vara så enkelt som möjligt för så många som möjligt att fullgöra sina skyldigheter samt att ta del av förvaltningens service. Detta övergripande mål ska uppnås med hjälp av insatser inom fyra olika områden. Ett av de insatsområden som identifieras i handlingsplanen är regelverk för myndighetsövergripande samverkan och informationshantering.

För att stärka utvecklingen av e-förvaltningen och skapa goda förutsättningar för myndighetsövergripande samordning inrättade regeringen i mars 2009 en delegation för e-förvaltning (dir. 2009:19). E-delegationen ska bl.a. koordinera de statliga myndigheternas it-baserade utvecklingsprojekt och följa upp deras effekter.

Nästan varje gång elektronisk informationsöverföring mellan myndigheter ska införas, ändras eller utökas måste ändringar göras i de aktuella registerförfattningarna. Vidare måste komplicerade överväganden göras enligt offentlighets- och sekretesslagen, och även den lagen kan behöva ändras. Om de grundläggande reglerna i tryckfrihetsförordningen och offentlighets- och sekretesslagen samt den principiella uppbyggnaden av registerförfattningarna inte är anpassade till varandra – utifrån de olika intressen dessa bestämmelser avser att skydda – blir det svårt att i ett enskilt lagstiftningsärende om elektronisk informationsöverföring mellan två eller flera myndigheter hitta en lösning som är tillfredsställande från integritets-, effektivitets- och öppenhetssynpunkt.

För att ytterligare kunna effektivisera förvaltningen med hjälp av modern informationsteknik är det därför viktigt dels att respektive regelverk är väl genomtänkt och så enkelt som möjligt att tillämpa, dels att dessa regelverk är förenliga med varandra. Mot denna bakgrund finns det behov av att göra en samlad översyn av dessa regelverk i relevanta delar. Med hänsyn till regelverkens komplexa natur och till att såväl Europarådet som EU ser över sina respektive dataskyddsregler lämnas inledningsvis en redogörelse för Sveriges internationella åtaganden och gällande svensk rätt på de aktuella områdena.

Internationella åtaganden

Europarådets dataskyddskonvention

De dataskyddsregler som antagits inom ramen för Europarådet finns i första hand i den europeiska konventionen om skydd för enskilda vid automatisk databehandling av personuppgifter (CETS 108), den s.k. dataskyddskonventionen, och dess tilläggsprotokoll. Konventionen kompletteras av ett antal av ministerkommittén antagna rekommendationer om hur personuppgifter bör behandlas inom olika områden. Sverige har, i likhet med övriga medlemsstater i EU, anslutit sig till dataskyddskonventionen. Under 2010 har Europarådet inlett en översyn av denna konvention.

EU:s dataskyddsreglering och det svenska genomförandet

Inom den f.d. första pelaren inom EU, som bl.a. innefattar den inre marknaden, preciseras och stärks Europarådets dataskyddskonvention genom Europaparlamentets och rådets direktiv 95/46/EG om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter, det s.k. dataskyddsdirektivet. Syftet med dataskyddsdirektivet är dels att garantera en hög skyddsnivå när det gäller enskilda personers fri- och rättigheter med avseende på behandling av personuppgifter, dels att denna skyddsnivå ska vara likvärdig i alla medlemsstater så att staterna inte ska kunna hindra det fria flödet av personuppgifter inom EU med hänvisning till sina respektive dataskyddsregleringar. Inom den f.d. tredje pelaren, som innefattar det polisiära och straffrättsliga samarbetet, gäller rambeslut 2008/977/RIF om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete, det s.k. dataskyddsrambeslutet.

Dataskyddsdirektivet är införlivat i den nationella lagstiftningen genom personuppgiftslagen (1998:204). Denna lag innehåller generella regler som, med vissa undantag, ska tillämpas i hela samhället av både myndigheter och enskilda. Den är dock subsidiär i förhållande till annan lag eller förordning. Behov av undantag och preciseringar på olika områden kan därmed tillgodoses genom särreglering i s.k. registerförfattningar. En sådan särreglering får dock inte stå i strid med dataskyddskonventionen, dataskyddsdirektivet

eller dataskyddsrambeslutet. Möjligheten att i en registerförfattning föreskriva särskilda bestämmelser för en viss typ av verksamhet har utnyttjats flitigt i den nationella lagstiftningen och det finns uppskattningsvis ca 200 registerförfattningar, t.ex. polisdatalagen (2010:361) och patientdatalagen (2008:355).

Frågan om hur dataskyddsrambeslutet ska genomföras i Sverige har utretts av en särskild utredare (dir. 2010:17). Denne har lämnat förslag till genomförande i delbetänkandet Dataskydd vid europeiskt polisiärt och straffrättsligt samarbete (SOU 2011:20). Betänkandet bereds inom Regeringskansliet.

En översyn av EU:s dataskyddsreglering

Genom Lissabonfördraget har det skett vissa förändringar av betydelse för dataskyddsregleringen inom EU. Den grundläggande rätten till skydd av personuppgifter regleras i artikel 8 i EU:s stadga om de grundläggande rättigheterna, vilken har gjorts rättsligt bindande. I artikel 16 i fördraget om EU:s funktionssätt anges vidare att Europaparlamentet och rådet – i enlighet med det ordinarie lagstiftningsförfarandet – ska fastställa bestämmelser om skydd för enskilda personer vid behandling av personuppgifter hos unionens institutioner, organ och byråer och i medlemsstaterna, när dessa utövar verksamhet som omfattas av unionsrättens tillämpningsområde, samt om den fria rörligheten för sådana uppgifter. Denna bestämmelse ger således en rättslig grund för reglering av personuppgiftsskydd i alla verksamheter som omfattas av EU-rätten.

EU-kommissionen har i ett meddelande, ”Ett samlat grepp på skyddet av personuppgifter i Europeiska unionen” (KOM [2010] 609), aviserat en strategi för en översyn av EU:s dataskyddsreglering. I meddelandet konstateras att den teknologiska utvecklingen och globaliseringen har medfört att det finns skäl att se över EU:s dataskyddsregelverk för att se till att det fortfarande erbjuder ett tillräckligt skydd. Vidare konstaterar kommissionen att många intressenter har framfört att det – trots den EU-rättsliga regleringen – fortfarande finns skillnader på nationell nivå som utgör ett hinder mot den inre marknaden. Kommissionen betonar därför behovet av ytterligare harmonisering. Kommissionen framhåller också behovet av ett heltäckande dataskyddsregelverk som,

till skillnad från dataskyddsdirektivet, även omfattar den f.d. tredje pelaren. I meddelandet anges att kommissionen kommer att lägga fram förslag till lagstiftning rörande den övergripande rättsliga ramen för personuppgiftsskydd under 2011.

Gällande nationell rätt

Den svenska grundlagsregleringen avseende skydd för personuppgifter

Tidigare har det i 2 kap. 3 § andra stycket regeringsformen (RF) föreskrivits att varje medborgare, i den utsträckning som närmare anges i lag, ska skyddas mot att hans eller hennes personliga integritet kränks genom att uppgifter om honom eller henne registreras med hjälp av automatisk databehandling. Bestämmelsen utgjorde inte något individuellt rättighetsskydd för enskilda, utan innebar endast att lagstiftaren var skyldig att i lag upprätthålla någon form av integritetsskydd i fråga om automatiserad behandling av personuppgifter.

Den 1 januari 2011 ersattes nämnda bestämmelse av en ny bestämmelse i 2 kap. 6 § andra stycket RF, enligt vilken var och en gentemot det allmänna är skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Begränsningar av denna fri- och rättighet får dock enligt 2 kap. 20 § första stycket 2 RF under vissa förutsättningar göras i lag. I en övergångsbestämmelse anges att äldre föreskrifter som innebär betydande intrång i den personliga integriteten behåller sin giltighet, dock längst t.o.m. den 31 december 2015. Grundlagsändringen medför bl.a. att viss personuppgiftsbehandling som för närvarande regleras i förordning i framtiden måste regleras i lag.

Offentlighetsprincipen

Allmänhetens möjlighet till insyn i den offentliga förvaltningen är av avgörande betydelse för en väl fungerande demokrati. Sedan 1766 har denna grundläggande rättighet – offentlighetsprincipen – varit reglerad i den svenska grundlagen. Offentlighetsprincipen innebär att allmänheten och massmedierna ska ha möjlighet till insyn i

statens och kommunernas verksamhet. Offentlighetsprincipen kommer till uttryck på olika sätt, exempelvis genom yttrande- och meddelarfrihet för tjänstemän, genom domstolsoffentlighet och genom offentlighet vid beslutande församlingars sammanträden. När det mer allmänt talas om offentlighetsprincipen åsyftas emellertid ofta i första hand reglerna om allmänna handlingars offentlighet i 2 kap. TF.

Med *handling* förstås enligt 2 kap. 3 § första stycket TF framställningar i skrift eller bild som kan uppfattas utan tekniskt hjälpmedel, dvs. handlingar i traditionell form. Med handling förstås därutöver upptagningar som kan läsas, avlyssnas eller på annat sätt uppfattas endast med tekniskt hjälpmedel. För att det ska finnas en rätt att ta del av en handling hos en myndighet krävs för det första att handlingen *förvaras* hos myndigheten. För det andra krävs att handlingen har nått ett sådant stadium i handläggningen att den är att betrakta som *allmän*. En handling måste därför antingen vara *inkommen* till eller *upprättad* hos myndigheten för att en rätt till insyn ska föreligga (2 kap. 6 och 7 §§ TF).

Den som önskar ta del av en allmän handling har rätt att göra detta på två olika sätt. Personen i fråga kan antingen avgiftsfritt ta del av handlingen genom att myndigheten tillhandahåller den på stället (2 kap. 12 § TF) eller mot avgift få den utlämnad till sig i avskrift eller kopia (2 kap. 13 § TF). En upptagning för automatiserad behandling behöver dock aldrig lämnas ut i annan form än utskrift i större utsträckning än vad som följer av lag. Syftet med detta s.k. utskriftsundantag är att förhindra att utlämnade uppgifter behandlas automatiserat på ett sätt som kan medföra otillbörliga integritetsintrång (prop. 1973:33 s. 85 f.).

Potentiella handlingar och färdiga elektroniska handlingar

Som nämns ovan kan endast de handlingar som förvaras hos myndigheten omfattas av handlingsoffentlighet. En upptagning anses enligt 2 kap. 3 § andra stycket TF *förvarad* hos myndigheten om upptagningen är tillgänglig för myndigheten med tekniskt hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas, avlyssnas eller på annat sätt uppfattas. För att närmare kunna avgöra om en upptagning för automatiserad behandling

är tillgänglig för myndigheten brukar en uppdelning göras mellan potentiella (elektroniska) handlingar och färdiga elektroniska handlingar.

En *potentiell handling*, dvs. en sammanställning av uppgifter som en myndighet har tekniska möjligheter att göra, är enligt 2 kap. 3 § andra stycket sista meningen TF förvarad hos myndigheten om denna kan göra sammanställningen tillgänglig med ”rutinbetonade åtgärder” (prop. 1975/76:160 s. 90). En sådan sammanställning anses dock inte vara förvarad hos myndigheten i tryckfrihetsförordningens mening om sammanställningen innehåller personuppgifter och myndigheten enligt lag eller förordning saknar befogenhet att göra sammanställningen tillgänglig. Detta framgår av den s.k. begränsningsregeln i 2 kap. 3 § tredje stycket TF. Med personuppgifter avses all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet. Om myndigheten sålunda saknar befogenhet att ta fram vissa upplysningar ur t.ex. ett personregister är dessa upplysningar inte allmänna handlingar hos myndigheten. Syftet med begränsningsregeln är att hindra allmänheten från att kunna göra anspråk på att få ta del av information hos myndigheten som myndigheten själv, av hänsyn till enskildas personliga integritet, är förhindrad att använda sig av. Begränsningsregeln gäller alltså även om sammanställningen kan tas fram med rutinbetonade åtgärder.

En *färdig elektronisk handling*, vilken är tillgänglig för myndigheten i uppfattbar form med tekniskt hjälpmedel som myndigheten själv utnyttjar, t.ex. en PDF-fil eller ett e-postmeddelande, anses förvarad hos myndigheten trots att det kan krävas mer än rutinbetonade åtgärder för att göra handlingen tillgänglig (prop. 2001/02:70 s. 20 f.). Färdiga elektroniska handlingar omfattas inte heller av begränsningsregeln.

En upptagning anses *inkommen* till en myndighet när den gjorts tillgänglig för myndigheten på det sätt som anges i 2 kap. 3 § andra stycket TF, dvs. med tekniskt hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas, avlyssnas eller på annat sätt uppfattas (2 kap. 6 § första stycket TF).

Begränsningsregelns närmare innebörd

Begränsningsregeln i 2 kap. 3 § tredje stycket TF innebär att dataskyddsbestämmelser i lag eller förordning får betydelse för hur omfattande begreppet ”allmän handling” är i praktiken.

Enligt dataskyddsdirektivet och personuppgiftslagen får personuppgifter bara samlas in för särskilda, uttryckligt angivna och berättigade ändamål (9 § första stycket c personuppgiftslagen). Enligt den s.k. finalitetsprincipen får en personuppgift inte behandlas för ett ändamål som är oförenligt med det ändamål för vilket uppgiften samlades in (9 § första stycket d). I förarbetena till personuppgiftslagen har dock uttalats att en myndighets utlämnande av personuppgifter med stöd av offentlighetsprincipen inte kan anses oförenligt med de ändamål för vilket uppgifterna ursprungligen samlades in (prop. 1997/98:44 s. 44). Regler om s.k. ändamålsbegränsningar, dvs. bestämmelser i registerförfattningar om för vilka ändamål myndigheten får behandla uppgifterna, anses inte heller inskränka myndighetens skyldighet enligt offentlighetsprincipen att sammanställa personuppgifter (prop. 2007/08:126 s. 120 f. och prop. 2007/08:160 s. 66 f.). Sistnämnda ställningstagande harmonierar väl med det s.k. efterfrågeförbudet i 2 kap. 14 § tredje stycket TF, av vilket det följer att en myndighet inte får fråga någon som begär ut en allmän handling vem han eller hon är eller vilket syfte han eller hon har med sin begäran, i större utsträckning än vad som behövs för att myndigheten ska kunna göra en sekretessprövning.

Så kallade sökbegränsningar, dvs. förbud i lag eller förordning mot att söka fram uppgifter eller göra sammanställningar med hjälp av vissa sökord, är dock i vissa fall avgörande för vilka sammanställningar som utgör allmänna handlingar. Det står nämligen klart att om den myndighet som förvarar en upptagning för automatiserad behandling under inga omständigheter får göra sammanställningar av uppgifter ur upptagningen med hjälp av vissa sökord har inte heller allmänheten rätt att ta del av en sådan sammanställning. Vissa sökbegränsningar som inte är absoluta utan tillåter sökning under särskilt angivna förutsättningar har dock ansetts sakna betydelse för frågan om sammanställningen utgör en allmän handling (se 3 kap. 6–7 §§ polisdatalagen [2010:361] och prop. 2009/10:85 s. 154 f., jfr prop. 2001/02:70 s. 23).

Sekretess

Rätten att ta del av en allmän handling gäller inte utan undantag. Denna rätt får dock begränsas endast om det är påkallat med hänsyn till vissa i 2 kap. 2 § TF uppräknade intressen. Sådan begränsning ska anges i en särskild lag. Den lag som avses är offentlighets- och sekretesslagen. I denna lag finns bestämmelser om sekretess som syftar till att skydda såväl allmänna som enskilda intressen.

Enligt 8 kap. 1 och 2 §§ OSL gäller sekretess inte bara i förhållande till allmänheten, utan också mellan myndigheter samt mellan olika verksamhetsgrenar inom en myndighet när de är att betrakta som självständiga i förhållande till varandra. Offentlighets- och sekretesslagen innehåller dock även sekretessbrytande regler. Som exempel kan nämnas 10 kap. 28 § första stycket OSL, som anger att sekretess inte hindrar att uppgift lämnas till en annan myndighet om uppgiftsskyldighet följer av lag eller förordning.

Förhållandet mellan bestämmelser om direktåtkomst och sekretessbrytande regler

Bestämmelser om direktåtkomst i registerförfattningar brukar formuleras så att en myndighet har rätt att få ha direktåtkomst till vissa uppgifter hos en annan myndighet. Sådana bestämmelser innebär dock bara att lagstiftaren eller regeringen ger den utlämnande myndigheten rätt att bevilja den mottagande myndigheten direktåtkomst till de nämnda uppgifterna, om den utlämnande myndigheten bedömer att säkerhetsfrågor m.m. kan lösas på ett tillfredsställande sätt.

Bestämmelser om direktåtkomst anses inte ha en sekretessbrytande effekt enligt offentlighets- och sekretesslagen (se t.ex. prop. 2004/05:164 s. 83). Det beror på att bestämmelser om direktåtkomst har en annan funktion än de sekretessbrytande reglerna. Sekretessbrytande regler anger i vilken mån sekretessbelagda uppgifter överhuvudtaget får lämnas från en myndighet till en annan. Bestämmelser om direktåtkomst tar sikte på formen för utlämnandet. På grund av de sammanställningsmöjligheter och möjligheter till spridning av uppgifter som en automatiserad behandling erbjuder anses det vara mer känsligt från integritetssynpunkt att lämna ut uppgifter elektroniskt än på papper. En myndighet kan

således enligt en bestämmelse om uppgiftsskyldighet ha skyldighet att lämna ut vissa uppgifter till en annan myndighet, men den mottagande myndigheten kanske bara har rätt att ha direktåtkomst till vissa av dessa uppgifter. Om tanken är att en myndighet ska få ha direktåtkomst till uppgifter som omfattas av sekretess hos en annan myndighet måste bestämmelsen om direktåtkomst kompletteras med en sekretessbrytande bestämmelse.

Det är vanligt att registerförfattningar stadgar att en myndighet får ha direktåtkomst till vissa angivna typer av uppgifter hos en annan myndighet beträffande personer *som är aktuella i ärenden hos den mottagande myndigheten*. Detta innebär att myndigheten bara får söka efter uppgifter om en person efter det att personen har blivit aktuell i ett ärende hos myndigheten. Rent tekniskt måste dock myndigheten ha möjlighet att ta del av sådana uppgifter beträffande *alla* personer som är registrerade hos den utlämnande myndigheten, eftersom den mottagande myndigheten inte i förväg kan veta vilka personer som kan komma att bli aktuella i ärenden hos myndigheten. Med hänsyn härtill har tolkningen av begränsningsregeln i 2 kap. 3 § tredje stycket TF behandlats i flera lagstiftningsärenden rörande elektroniskt informationsutbyte mellan myndigheter. Det har då konstaterats att som huvudregel blir sådan överskottsinformation som en myndighet rent tekniskt har tillgång till hos en annan myndighet i samband med direktåtkomst att betrakta som en allmän handling hos den mottagande myndigheten, även om den mottagande myndigheten enligt den tillämpliga registerförfattningen vid ett givet tillfälle inte har rätt att behandla uppgifterna för egen del. Det sagda gäller dock inte uppgifter som omfattas av ett absolut s.k. sökförbud enligt den aktuella registerförfattningen (prop. 2007/08:126 s. 120 f. och prop. 2007/08:160 s. 66 f.). De sekretessbrytande regler som ska möjliggöra uppgiftsutbytet måste bl.a. av detta skäl normalt omfatta även sådan överskottsinformation som den utlämnande myndigheten rent tekniskt gör tillgänglig för den mottagande myndigheten i samband med direktåtkomst (prop. 2007/08:160 s. 70 f.). Sådana sekretessbrytande bestämmelser har således ett relativt omfattande tillämpningsområde.

De sekretessbrytande bestämmelserna kan kompletteras av andra bestämmelser som innebär ett integritetsskydd för den enskilde. Bestämmelser om direktåtkomst som anger att handläggarna hos

den mottagande myndigheten bara får ta del av uppgifter som avses i de sekretessbrytande bestämmelserna beträffande personer som är aktuella i ärenden hos den mottagande myndigheten utgör ett sådant skydd. Den tekniska utvecklingen har även lett till att det numera är möjligt att inom den mottagande myndigheten införa tekniska spärrar mellan teknikavdelningen och handläggarna som t.ex. medför att en handläggare inte bara är rättsligt utan även tekniskt förhindrad att söka på andra personer än sådana som är aktuella hos myndigheten. Integritetsskyddande bestämmelser i den mottagande myndighetens registerförfattning och i personuppgiftslagen om säkerhet m.m. samt bestämmelsen om överföring av sekretess i 11 kap. 4 § OSL (se närmare nedan) utgör också ett integritetsskydd.

På grund av att sekretessbrytande regler som införs med anledning av direktåtkomst har en så vid utformning har regeringen anfört att en mottagande myndighet i sin arbetsordning bör ange vilka personer som för vilka syften har behörighet att för myndighetens räkning ta del av de uppgifter som anges i de sekretessbrytande bestämmelserna. Sådana föreskrifter fyller beträffande utlämnande via telefon eller brev samma integritetsskyddande funktion som ovan beskrivna bestämmelser om direktåtkomst gör när det gäller elektroniskt inhämtande av information (prop. 2007/08:160 s. 72). I ett senare lagstiftningsärende har regeringen anfört att integritetsskyddet blir ännu starkare om det på lag- eller förordningsnivå i stället tas in två olika typer av sekretessbrytande bestämmelser, dels en sekretessbrytande bestämmelse som tar sikte på uppgiftslämnande i enskilda fall och som kan användas vid utlämnande av uppgifter t.ex. via telefon eller mejl, dels en vidare sekretessbrytande bestämmelse som bara gäller vid direktåtkomst. Den förra typen av sekretessbrytande regel kan behövas t.ex. om det på grund av tekniska problem tillfälligt inte går att använda sig av direktåtkomst (prop. 2010/11:78 s. 21).

Förhållandet mellan direktåtkomst, begreppet allmän handling och sekretessbestämmelser

Eftersom huvudregeln är att s.k. överskottsinformation som blir tekniskt tillgänglig för den mottagande myndigheten i samband med direktåtkomst blir allmän handling hos den mottagande myn-

digheten, kan allmänheten begära att få ta del av uppgifter hos den mottagande myndigheten även i situationer när den mottagande myndigheten av integritetsskäl bör vara förhindrad att ens titta på uppgifterna i fråga. En sådan situation förutsågs i samband med antagandet av patientdatalagen. Vid sammanhållen journalföring mellan flera olika vårdgivare får en vårdgivare enligt patientdatalagen inte ta del av uppgifter som andra vårdgivare lagt in i systemet om inte patienten samtycker till det. Eftersom uppgifter som är tekniskt tillgängliga hos en vårdgivare som huvudregel är en allmän handling där kan dock enskilda begära att få ut dem där, oaktat att vårdgivaren inte har rätt att titta på uppgifterna enligt patientdatalagen. Med anledning av att en sekretessprövning normalt kräver att befattningshavare granskar den handling som begärs ut föreslogs i lagstiftningsärendet en ny sekretessbestämmelse av innebörd att det gäller absolut sekretess för uppgifter som en vårdgivare har teknisk tillgång till, men som vårdgivaren inte har rätt att titta på enligt patientdatalagen. Denna konstruktion innebär att hälso- och sjukvårdspersonalen vid begäran om utfående av sådana uppgifter inte behöver ta del av de begärda uppgifterna för att kunna avgöra sekretessfrågan (25 kap. 2 § OSL och prop. 2007/08:126 s. 126 f.).

Eftersom det inte alltid finns sekretessbestämmelser som hos en mottagande myndighet är tillämpliga på sådan överskottsinformation som myndigheten får teknisk tillgång till vid direktåtkomst har det, för det fall uppgifterna omfattas av sekretess hos den utlämnande myndigheten, införts en bestämmelse om överföring av sekretess vid direktåtkomst (11 kap. 4 § OSL, prop. 2007/08:160 s. 72 f.). Sistnämnda bestämmelse kompletteras av en undantagsbestämmelse i 11 kap. 8 § OSL. Undantagsbestämmelsen stadgar att sekretess som är direkt tillämplig hos den mottagande myndigheten, s.k. primär sekretess, har företräde framför överförd sekretess och det oavsett om den primära sekretessen är starkare eller svagare än den överförda sekretessen. Även uttryckliga undantag från den primära sekretessbestämmelsens tillämpningsområde har företräde framför den överförda sekretessen. Med hänsyn till denna undantagsbestämmelse gjordes i propositionen bedömningen att bestämmelsen om överföring av sekretess vid direktåtkomst inte rubbade den grundläggande principen i sekretesslagstiftningen att sekretessbehovet alltid ska vägas mot insynsintresset samt att denna

avvägning kan utfalla på skilda sätt hos olika myndigheter och inom olika områden (prop. 2007/08:160 s. 34 och 75 f.). Denna princip innebär således att en och samma uppgift kan vara hemlig hos den utlämnande myndigheten och offentlig hos den mottagande myndigheten.

Om uppgifterna har ett svagare sekretesskydd hos den mottagande myndigheten än hos den utlämnande myndigheten kan dock undantagsregeln i 11 kap. 8 § OSL, beroende på hur sekretesskyddet hos den mottagande myndigheten är konstruerat, i vissa fall medföra att stora delar av den utlämnande myndighetens databas får ett mycket svagare sekretesskydd hos den mottagande myndigheten, trots att detta svagare skydd är motiverat bara beträffande de uppgifter som faktiskt används i den mottagande myndighetens verksamhet. Detta är inte lämpligt från integritetssynpunkt. I en sådan situation måste ytterligare överväganden göras för att åstadkomma ett skydd för sådan överskottsinformation som i och för sig är tekniskt tillgänglig för den mottagande myndigheten men som denna inte använder i sin verksamhet (prop. 2007/08:160 s. 95).

Elektroniskt utlämnande av allmänna handlingar till allmänheten

Som nämns tidigare följer av det s.k. utskriftsundantaget i tryckfrihetsförordningen att en myndighet inte är skyldig att i större utsträckning än vad som följer av lag lämna ut en upptagning för automatiserad behandling i annan form än utskrift (2 kap. 13 § TF). Bestämmelsen syftar till att minimera riskerna för otillbörliga integritetsintrång. Av förordningen (2003:234) om tiden för tillhandahållande av domar och beslut, m.m. framgår att en handling får skickas med telefax eller elektronisk post eller på annat sätt tillhandahållas i elektronisk form, om det är lämpligt (10 §).

E-offentlighetskommittén fick i uppdrag att överväga om det i dåvarande sekretesslagen (1980:100) eller i annan lag bör införas en bestämmelse som medför en generell skyldighet för myndigheter att lämna ut elektroniskt lagrade allmänna handlingar i elektronisk form. I betänkandet Allmänna handlingar i elektronisk form (SOU 2010:4) anförde kommittén att en utgångspunkt för kommitténs överväganden är att det långsiktiga målet bör vara att myndigheterna bör ha en i lag reglerad skyldighet att – i den mån det inte

finns särskilda förbud mot det i lag eller förordning – lämna ut allmänna handlingar i elektronisk form om sökanden så önskar. Kommittén ansåg dock att en sådan skyldighet inte kan införas förrän en grundlig genomgång och bearbetning har genomförts av samtliga registerförfattningar (s. 306 f.).

Uppdraget

Bör definitionen av begreppet ”allmän handling” ändras?

Som framgår ovan innebär den nuvarande regleringen i tryckfrihetsförordningen att s.k. överskottsinformation som blir tekniskt tillgänglig för den mottagande myndigheten i samband med direktåtkomst som huvudregel blir allmän handling hos den myndigheten. Frågan är om de skillnader som finns mellan den utlämnande myndighetens och den mottagande myndighetens hantering av de berörda uppgifterna gör att det finns skäl att ändra denna ordning.

Skälet till att enskilda har rätt att ta del av potentiella allmänna handlingar är att det anses följa av den s.k. likställighetsprincipen att enskilda bör ha samma möjligheter som aktuell myndighet att ta del av sammanställningar av uppgifter ur upptagningar för automatiserad behandling (prop. 1975/76:160 s. 90). Begränsningsregeln i 2 kap. 3 § tredje stycket TF utgör således ett uttryck för likställighetsprincipen.

När en myndighet har samlat in personuppgifter för särskilda, uttryckligt angivna och berättigade ändamål enligt personuppgiftslagen och tillämplig registerförfattning, saknar frågan om för vilka ändamål myndigheten sedan får behandla uppgifterna relevans för enskildas rätt att begära ut sammanställningar av uppgifterna. När en annan myndighet därefter ges direktåtkomst till vissa av dessa uppgifter, måste den mottagande myndigheten, på det sätt som har beskrivits ovan, ofta rent tekniskt få tillgång till fler uppgifter än vad rätten till direktåtkomst avser. Uppgifter som genom direktåtkomst har överförts till den mottagande myndigheten i ett enskilt fall, t.ex. i ett ärende, anses insamlade hos den mottagande myndigheten enligt personuppgiftslagen och tillämplig registerförfattning. Överskottsinformation som den mottagande myndigheten rent tekniskt har tillgång till i samband med direktåtkomst, dvs. sådana uppgifter som den mottagande myndigheten vid det aktuella

tillfället inte har rätt att behandla enligt den tillämpliga registerförfattningen eftersom myndigheten inte har några ärenden rörande dessa personer, anses däremot inte insamlad i personuppgiftslagens mening hos den mottagande myndigheten. Detsamma gäller uppgifter som visserligen avser personer som är aktuella i ärenden hos myndigheten, men där uppgifterna ännu inte faktiskt har överförts till verksamheten.

Eftersom likställighetsprincipen utgör skälet för enskildas rätt att ta del av potentiella allmänna handlingar, kan det ifrågasättas om uppgifter som den mottagande myndigheten vid ett givet tillfälle inte har rätt att ta del av och som inte heller kan anses insamlade hos den myndigheten enligt personuppgiftslagen och tillämplig registerförfattning ska anses förvarade hos den myndigheten och därmed utgöra inkomna allmänna handlingar hos den myndigheten. Vidare medför i regel inte det faktum att s.k. överskottsinformation utgör allmän handling hos den mottagande myndigheten någon utökad insyn för allmänheten, eftersom överskottsinformationen enligt en komplicerad reglering i offentlighets- och sekretesslagen ofta omfattas av en minst lika stark sekretess hos den mottagande myndigheten som hos den utlämnande myndigheten.

Mot den angivna bakgrunden bör utredaren överväga om överskottsinformation i form av färdiga eller potentiella elektroniska handlingar som i samband med elektroniskt informationsutbyte enbart av tekniska skäl görs tillgänglig för den mottagande myndigheten, även i fortsättningen bör anses utgöra allmänna handlingar hos den mottagande myndigheten eller om det finns skäl att ändra definitionen av begreppet allmän handling i detta avseende.

För det fall utredaren finner att tryckfrihetsförordningen bör ändras ska utredaren lämna författningsförslag samt förslag till konsekvensändringar i offentlighets- och sekretesslagen. Förhållandet mellan tystnadsplikten (3 kap. 1 § OSL) och de möjligheter som finns att införa tekniska spärrar, kryptering m.m. beträffande både personalen hos den mottagande myndighetens teknikavdelning och handläggarna hos den myndigheten ska särskilt beaktas.

Om utredaren finner att grundlagen inte bör ändras ska utredaren utvärdera om de bestämmelser som förts in i offentlighets- och sekretesslagen med anledning av den nuvarande ordningen (11 kap. 4 § och 25 kap. 2 § OSL) har en lämplig utformning eller

om de bör justeras samt, om så anses vara fallet, lämna författningsförslag.

Bör åtskillnaden mellan olika former av elektroniskt utlämnande bibehållas?

Uppgifter kan lämnas ut elektroniskt även på andra sätt än genom direktåtkomst. I registerförfattningarna brukar begreppet ”utlämnande på medium för automatiserad behandling” användas.

Med direktåtkomst menas vanligtvis att någon har direkt tillgång till någons databaser eller register och på egen hand kan söka efter information, dock utan att kunna påverka innehållet i databasen eller registret. Begreppet brukar också anses innefatta att den som är ansvarig för databasen eller registret inte har någon kontroll över vilka uppgifter som mottagaren vid ett visst tillfälle tar del av (prop. 2004/05:164 s. 83). Från integritetssynpunkt har det därför ansetts angeläget att frågor om tillgång till uppgifter genom direktåtkomst särskilt regleras i registerlagstiftningen (prop. 2000/01:129 s. 74, prop. 2001/02:144 s. 35 f. och prop. 2005/06:52 s. 8).

Med begreppet utlämnande på medium för automatiserad behandling avses i nuvarande författningar utlämnande av uppgifter i elektronisk form på en rad olika sätt, t.ex. genom användning av e-post, genom utlämnande på USB-minne eller genom automatiserad överföring med tidsfördröjning från ett datorsystem till ett annat (prop. 2007/08:160 s. 58). Att utlämnande sker på medium för automatiserad behandling innebär i regel att informationen lämnas ut i elektronisk form på ett sådant sätt att mottagaren kan bearbeta informationen (prop. 2002/03:135 s. 97 och prop. 2004/05:164 s. 82).

Den tekniska utvecklingen har inneburit att det numera finns betydligt fler sätt att överföra uppgifter elektroniskt än tidigare och nya åtkomstmetoder tillkommer alltjämt. Detta har medfört att det uppfattas som oklart hur begreppen direktåtkomst och utlämnande på medium för automatiserad behandling ska tillämpas på modernare metoder för informationsutbyte. Gränsdragningsproblematiken illustreras bl.a. i en rapport som har tagits fram av E-delegationens expertgrupp för rättsliga frågor (Vägledning för direktåtkomst och utlämnande på medium för automatiserad behandling). De aktuella begreppen används inte heller på ett enhetligt sätt i de olika

registerförfattningarna och utöver nu nämnda begrepp förekommer andra begrepp, t.ex. ”elektronisk åtkomst” (SOU 2010:4 s. 364 f.).

Mot den angivna bakgrunden ska utredaren analysera vilka effektivitetsvinster och integritetsrisker som är förknippade med olika former av elektroniskt informationsutbyte samt ta ställning till om det finns skäl att i registerförfattningarna upprätthålla en skillnad mellan direktåtkomst och andra former av elektroniskt utlämnande eller om denna åtskillnad bör utmönstras. Om utredaren anser att en åtskillnad mellan olika former av elektroniskt utlämnande även i fortsättningen bör upprätthållas, ska denne lämna förslag på vilka begrepp som bör användas samt hur dessa bör definieras.

En mall för registerförfattningar samt modellregleringar

Flera utredningar, bl.a. 2005 års informationsutbytesutredning, Integritetsskyddskommittén, E-delegationen och E-offentlighetskommittén, har påtalat att registerförfattningarna behöver ses över. Den förstnämnda utredningen gjorde i betänkandet Utökat elektroniskt informationsutbyte (SOU 2007:45) den övergripande bedömningen att de befintliga registerförfattningarna bör ses över för att skapa förutsättningar för ett samordnat och enhetligt regelverk som främjar utvecklingen av elektronisk förvaltning och minskar riskerna för oacceptabla intrång i den personliga integriteten. Integritetsskyddskommittén redovisade i sitt betänkande Skyddet för den personliga integriteten (SOU 2007:22) den sammanfattande analysen att skyddet för den personliga integriteten väsentligt skulle förbättras om registerförfattningarna utformades enhetligare, tydligare och mer i överensstämmelse med sekretesslagstiftningen. E-delegationen har anfört att de för närvarande ca 200 registerförfattningarna saknar en sinsemellan enhetlig struktur och att olika begrepp används för att beskriva samma företeelse (t.ex. databas och register), samtidigt som samma begrepp förekommer i olika betydelser (t.ex. direktåtkomst och gallring). För att möjliggöra en utveckling i riktning mot en flexibel e-förvaltning anser E-delegationen att det krävs att registerförfattningarna är samordnade, enhetliga och tydliga samt att regelkonflikter mellan registerförfattningarna och offentlighets- och sekretesslagen undanröjs

(SOU 2009:86 s. 65 och SOU 2010:20 s. 17). Vidare har Datainspektionen sedan 2005 i sina årsredovisningar pekat på ett allt starkare behov av en översyn och ett samlat grepp när det gäller registerlagstiftningen inom statsförvaltningen. Även Riksrevisionen anser att registerförfattningarna bör ses över (RiR 2010:18 s. 64).

Regeringen anser, i likhet med nämnda utredningar samt Datainspektionen och Riksrevisionen, att registerförfattningarna bör ses över. Med hänsyn till det stora antalet författningar bör dock översynen ske etappvis.

Utredaren ska göra en översiktlig inventering av gällande registerförfattningar och inom tre olika verksamhetsområden närmare analysera hur dessa är uppbyggda och tillämpas. Vilka tre verksamhetsområden som särskilt ska analyseras kommer att anges av regeringen i tilläggsdirektiv, efter inhämtande av synpunkter från utredaren. Utredaren ska därefter utarbeta en generell modell för hur registerförfattningar bör struktureras, vilka begrepp som bör användas samt hur dessa begrepp bör definieras. Slutligen ska utredaren, med nämnda modell som mall, lämna konkreta förslag till registerförfattningar inom de tre verksamhetsområdena (s.k. modellregleringar).

Inom dessa tre områden ska utredaren även överväga vilka typer av allmänna handlingar som den eller de aktuella myndigheterna ska ha skyldighet att lämna ut elektroniskt samt lämna förslag till hur denna skyldighet bör regleras. Utredaren ska särskilt överväga om skyldigheten bör regleras i offentlighets- och sekretesslagen och specificeras i en ny bilaga till lagen, eventuellt i form av hänvisningar till de berörda registerförfattningarna. I denna del ska utredaren beakta de begränsningar som kan finnas med anledning av internationella åtaganden, jfr SOU 2011:20 s. 286.

Journalistförbundet har i en framställan till regeringen (Ju2006/4517/L6) anfört att den omfattande registerregleringen medför att undersökningar av stora material försvåras eller omöjliggörs, vilket hotar medias möjligheter att granska hur makten utövas och förvaltas. Journalistförbundet anser bl.a. att bestämmelser om sökförbud och utlämnande på medium för automatiserad behandling begränsar möjligheterna till sådan granskning. Utredaren ska under arbetet belysa denna problematik och utforma sina förslag efter en avvägning mellan intresset av skydd för den personliga integriteten och intresset av insyn i myndigheternas verksamhet.

Gäller sökbegränsningar som tar sikte på den utlämnande myndigheten även för den mottagande myndigheten?

Som nämns tidigare innebär ett absolut sökförbud i en registerförfattning även en begränsning av vad som utgör allmän handling (2 kap. 3 § tredje stycket TF). Det står klart att ett sådant sökförbud i en registerförfattning har relevans för bedömningen av vilka sammanställningar av personuppgifter som anses utgöra allmänna handlingar hos den myndighet som registerförfattningen tar sikte på. Det är dock omdiskuterat vilken betydelse sökförbud i den utlämnande myndighetens registerförfattning har för bedömningen av frågan vilka sammanställningar av personuppgifter som utgör allmänna handlingar hos den mottagande myndigheten. I uppdraget ingår att ta ställning till vad som bör gälla i detta avseende.

Regelkonflikter

Enligt 6 kap. 5 § OSL ska en myndighet på begäran av en annan myndighet lämna uppgift som den förfogar över, om inte uppgiften är sekretessbelagd eller det skulle hindra ärendets behöriga gång. Denna skyldighet anses utgöra en precisering av den allmänna samverkansskyldighet som gäller för myndigheterna enligt 6 § förvaltningslagen (1986:223). Det har ifrågasatts om denna skyldighet står i strid med den s.k. finalitetsprincipen i dataskyddsdirektivet. Som nämns tidigare innebär denna princip att en personuppgift inte får behandlas för ett ändamål som är oförenligt med det ändamål för vilket uppgiften samlades in. Offentlighets- och sekretesskommittén anförde emellertid i sitt huvudbetänkande (SOU 2003:99 s. 231 f.) att regering och riksdag redan vid personuppgiftslagens tillkomst tagit ställning till att bestämmelsen i dåvarande 15 kap. 5 § sekretesslagen (nuvarande 6 kap. 5 § OSL) inte strider mot dataskyddsdirektivet. Enligt kommittén ska således ett utlämnande av uppgifter till en annan myndighet anses vara förenligt med finalitetsprincipen om utlämnandet är tillåtet enligt sekretesslagen. Kommittén ansåg dock att det skulle kunna uppstå en normkollision mellan 15 kap. 5 § sekretesslagen och en registerförfattning, om ändamålsregleringen i den senare författningen är utformad så att den utesluter en tillämpning av finalitetsprincipen. I en sådan

situation får enligt kommittén ändamålsregleringen i registerförfattningen anses utgöra lex specialis i förhållande till 15 kap. 5 § sekretesslagen och ett utlämnande av uppgifter i strid med ändamålsregleringen skulle därmed utgöra en otillåten behandling av uppgifterna. Enligt utredningen var det dock oklart om det fanns några registerförfattningar som på detta sätt uteslöt en tillämpning av finalitetsprincipen (s. 236 f.).

Såsom bl.a. Integritetsskyddskommittén har uppmärksammat förekommer det emellertid numera sådana uttömmande ändamålsregleringar som leder till att ett utlämnande av uppgifter mellan myndigheter som är tillåtet enligt offentlighets- och sekretesslagen är förbjudet enligt registerförfattningen (SOU 2007:22 s. 464 f.). Regeringen anser att utgångspunkten bör vara att ändamålsregleringar som utesluter en tillämpning av finalitetsprincipen inte ska förekomma. De förslag till registerförfattningar som utredaren lämnar ska även i övrigt harmoniera med tryckfrihetsförordningen, offentlighets- och sekretesslagen samt Sveriges internationella åtaganden.

En närliggande fråga har sin grund i det faktum att internationella avtal och sektorsspecifika EU-rättsakter ibland innehåller artiklar om att en myndighet bara får använda uppgifter som erhålls enligt avtalet respektive rättsakten för vissa angivna ändamål eller i viss verksamhet. Sådana bestämmelser kan avse även andra uppgifter än personuppgifter. I Sverige anses en sådan bestämmelse inte utgöra ett hinder mot utlämnande av uppgifter med stöd av offentlighetsprincipen. Däremot kan en sådan användningsbegränsning anses stå i konflikt med myndighetens skyldighet att överlämna uppgifter till andra myndigheter i enlighet med 6 kap. 5 § OSL. Någon generellt tillämplig eller konsekvent genomförd lösning på sistnämnda typ av regelkonflikt finns för närvarande inte i lagstiftningen. I 9 kap. 2 § OSL ges visserligen en upplysning om att användningsbegränsningar genomförts i vissa andra författningar. Uppräkningen är dock inte heltäckande och det finns dessutom inte någon formell koppling mellan denna bestämmelse och 6 kap. 5 § OSL (jfr prop. 1990/91:131 s. 25). De författningar som avses i 9 kap. 2 § OSL utgör visserligen inte registerförfattningar. Den beskrivna frågeställningen har dock en sådan betydelse för uppgiftsutbytet mellan myndigheter att den ändå bör utredas i detta sammanhang. Utredaren ska därför överväga om 6 kap. 5 § OSL

bör justeras så att den står i bättre överensstämmelse med förekomsten av nu nämnda användningsbegränsningar. Om utredaren finner att en sådan justering bör ske, ska författningsförslag lämnas.

Övrigt

Utredaren är oförhindrad att ta upp andra frågor än de som nämns i direktiven, om utredaren anser att dessa behöver regleras för att utredaren ska kunna fullgöra sitt uppdrag på ett tillfredsställande sätt.

Genomförande av uppdraget

Utredaren ska i ett delbetänkande redovisa sina ställningstaganden och eventuella förslag rörande dels tryckfrihetsförordningens definition av begreppet ”allmän handling”, dels frågan om det finns skäl att i registerförfattningar även i fortsättningen upprätthålla en skillnad mellan direktåtkomst och andra former av elektroniskt utlämnande. Regeringen kommer i tilläggsdirektiv, efter att ha inhämtat synpunkter från utredaren, att ange inom vilka tre verksamhetsområden som utredaren ska lämna konkreta förslag till registerförfattningar.

Under sitt arbete ska utredaren beakta den pågående översynen av såväl Europarådets som EU:s dataskyddsreglering. Utredaren ska hålla sig informerad om hur detta arbete fortskrider och hur det påverkar handlingsutrymmet när det gäller utformningen av den nationella lagstiftningen.

När det gäller frågan om definitionen av ”allmän handling” bör ändras ska utredaren samråda med en parlamentarisk referensgrupp.

Utredaren ska i uppdragets samtliga delar samråda med E-delegationen samt, i den utsträckning som utredaren finner det behövligt, med andra kommittéer och utredare som arbetar med närliggande frågeställningar. Utredaren ska också samråda med de fyra myndigheter som fått regeringens uppdrag att samordna och främja myndigheternas arbete med e-förvaltning, nämligen Skatteverket, Lantmäteriet, Transportstyrelsen och Bolagsverket (N2011/1368/ITP).

Utredaren ska bedöma de ekonomiska konsekvenserna av förslagen för det allmänna och för enskilda. Om förslagen kan förväntas leda till kostnadsökningar för det allmänna, ska utredaren föreslå hur dessa ska finansieras.

Delbetänkandet ska redovisas senast den 1 december 2012. Uppdraget ska slutredovisas senast den 1 december 2014.

(Justitiedepartementet)

Kommittédirektiv 2014:31

Tilläggsdirektiv till Informationshanteringsutredningen

Beslut vid regeringssammanträde den 6 mars 2014

Ändring av och förlängd tid för uppdraget

Utredningens uppdrag ändras. Uppdraget att analysera registerförfattningar inom tre olika verksamhetsområden och lämna förslag på registerförfattningar för dessa verksamheter samt att överväga vilka typer av allmänna handlingar som myndigheterna inom dessa verksamhetsområden ska vara skyldiga att lämna ut i elektronisk form utgår. Utredningen ska i stället koncentrera arbetet på att utreda förutsättningarna för att skapa en generell, enhetlig och samlad reglering för myndigheternas personuppgiftsbehandling och lämna författningsförslag till en sådan, med beaktande bl.a. av den pågående översynen inom Europeiska unionen av regleringen om skyddet för personuppgifter. Personuppgiftsbehandling inom den brottsbekämpande verksamheten omfattas inte av det uppdrag för utredningen som nu preciseras.

Uppdraget skulle ursprungligen redovisas den 1 december 2014. Utredningstiden förlängs. Uppdraget ska i stället redovisas senast den 30 januari 2015.

Utredningens nuvarande uppdrag

Med stöd av regeringens beslut den 6 oktober 2011 gav chefen för Justitiedepartementet en särskild utredare i uppdrag att se över den s.k. registerlagstiftningen och vissa därmed sammanhängande frågor i

syfte att skapa rättsliga förutsättningar för en effektivare e-förvaltning där såväl den enskildes rätt till personlig integritet som allmänhetens berättigade anspråk på insyn i den offentliga verksamheten tillgodoses (dir. 2011:86). Utredningen tog namnet Informationshanteringsutredningen (Ju 2011:11).

Den 11 januari 2013 lämnade utredningen delbetänkandet Överskottsinformation vid direktåtkomst (SOU 2012:90). I betänkandet redovisas bl.a. utredningens arbete med frågan om begreppet allmän handling i tryckfrihetsförordningen i förhållande till s.k. överskottsinformation vid myndigheters direktåtkomst till andra myndigheters elektroniskt lagrade personuppgifter.

I utredningens uppdrag att se över registerlagstiftningen ingår bl.a. att göra en översiktlig inventering av gällande registerförfattningar och närmare analysera hur dessa fungerar inom tre olika verksamhetsområden. Det anges i direktiven att regeringen i tilläggsdirektiv kommer att precisera vilka tre verksamhetsområden som närmare ska analyseras, efter att synpunkter inhämtats från utredaren. I uppdraget ingår även att utarbeta en generell modell för hur registerförfattningar bör struktureras, vilka begrepp som bör användas och hur begreppen bör definieras. Med modellen som mall ska utredningen lämna konkreta förslag till registerförfattningar inom de tre verksamhetsområdena. För dessa områden ska utredaren även överväga vilka typer av allmänna handlingar som berörda myndigheter ska ha skyldighet att lämna ut i elektronisk form och föreslå författningsreglering. Av direktiven framgår vidare att utredningen ska överväga ett antal särskilt angivna frågor, bl.a. om åtskillnaden mellan olika former av elektroniskt utlämnande bör behållas och om s.k. sökbegränsningar som tar sikte på en utlämnande myndighet gäller även för en mottagande myndighet.

Översynen av EU:s dataskyddsreglering

Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (EGT L 281, 23.11.1995, s. 31), förkortat dataskyddsdirektivet, har genomförts i Sverige genom bl.a. personuppgiftslagen (1998:204). Personuppgiftslagen är generellt tillämplig för all helt eller delvis

automatiserad behandling av personuppgifter och behandling av personuppgifter i manuella register. Den tillämpas dock inte om något annat följer av avvikande bestämmelser som finns i en annan lag eller i en förordning.

Rådets rambeslut 2008/977/RIF av den 27 november 2008 om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete (EUT L 350, 30.12.2008, s. 60), förkortat dataskyddsrambeslutet, har genomförts genom lagen (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen. Lagen gäller, med vissa begränsningar, för behandling av personuppgifter i verksamhet som har till syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller beivra brott eller verkställa straffrättsliga påföljder, bl.a. om uppgifterna överförts mellan en svensk myndighet och myndighet i en annan medlemsstat i EU eller ett EU-organ.

Sedan Lissabonfördraget trädde i kraft den 1 december 2009 finns i artikel 16 i fördraget om Europeiska unionens funktionssätt en ny rättslig grund för unionslagstiftning om skydd för personuppgifter. Den omfattar både EU:s inre marknad och det polisiära och straffrättsliga samarbetet mellan EU:s medlemsstater. I och med Lissabonfördragets ikraftträdande gäller vidare Europeiska unionens stadga för de grundläggande rättigheterna med bindande verkan för medlemsstaterna när dessa tillämpar unionsrätten (EUT C 326, 26.10.2012, s. 391). Av EU-domstolens praxis framgår att detta innebär att de rättigheter som garanteras i stadgan måste iakttas när en nationell lagstiftning omfattas av unionsrättens tillämpningsområde (C-617/10 Åkerberg Fransson, dom den 26 februari 2013). Av artikel 8 i stadgan följer att var och en har rätt till skydd av de personuppgifter som rör honom eller henne.

Den 25 januari 2012, dvs. efter att direktiven till utredningen beslutades, presenterade EU-kommissionen ett förslag till en genomgripande reform av EU:s regler om skydd för personuppgifter. Kommissionen har lämnat förslag till dels en förordning med en generell reglering av uppgiftsskyddet som ska ersätta dataskyddsdirektivet, dels ett direktiv om uppgiftsskydd i den brottsbekämpande verksamheten som ska ersätta dataskyddsrambeslutet. Förslaget till direktiv har dock ett bredare tillämpningsområde än rambeslutet och omfattar, utöver gränsöverskridande personuppgifts-

behandling, även rent nationell behandling av personuppgifter i sådan verksamhet (KOM [2012]10 och [2012]11).

Förhandlingarna om de båda förslagen pågår inom EU. Det är i nuläget oklart hur lång tid det kan ta innan de båda rättsakterna antas slutligt av Europaparlamentet och rådet. Förhandlingarna om direktivet har inte kommit lika långt som förhandlingarna om förordningen. Det är också oklart vilka effekter de nya reglerna kommer att få i Sverige. I förhandlingarna om direktivet vänder sig t.ex. flera medlemsstater mot att i unionsrätten reglera förutsättningarna för rent nationell behandling av personuppgifter på området. Om dataskyddsdirektivet ersätts av en EU-förordning kommer under alla förhållanden i vart fall personuppgiftslagen att behöva upphävas eller lagens tillämpningsområde snävas in avsevärt. I vilken utsträckning det kommer att finnas utrymme att behålla en sektorspecifik registerlagstiftning och i vilken mån det blir möjligt att komplettera EU-förordningen med generella nationella normer är för närvarande svårt att förutse. I förhandlingarna om dataskyddsförordningen förespråkar Sverige att regleringen ges formen av ett direktiv i stället för en förordning, men stödet för detta har visat sig vara svagt bland övriga medlemsstater. Mot den bakgrunden arbetar regeringen för att förordningen utformas på ett sätt som ger medlemsstaterna stor flexibilitet att precisera villkoren för behandlingen av personuppgifter främst inom den offentliga sektorn. För en sådan inriktning finns det ett brett stöd också bland övriga medlemsstater.

Ändring av uppdraget

Det är viktigt att översynen av registerlagstiftningen sker på ett sätt som är anpassat till det pågående arbetet inom EU med att reformera dataskyddsregleringen. Med beaktande av kommissionens förslag och det stöd som förefaller finnas inom EU för en dataskyddsreglering som ges formen av en förordning, kan utredningen i sitt fortsatta arbete inte längre utgå från att det kommer att vara möjligt att behålla en heltäckande och allmängiltig nationell författningsreglering om behandling av personuppgifter som på ett eller annat sätt kompletteras av sektorsvisa registerförfattningar. Mot den bakgrunden är det inte ändamålsenligt att utredningen ana-

lyserar registerförfattningarna inom tre olika verksamhetsområden och lämnar konkreta författningsförslag för dessa områden. I stället bör utredningen koncentrera sitt fortsatta arbete på att utreda förutsättningarna för att skapa en generell, enhetlig och – helt eller i vart fall delvis – samlad reglering för myndigheternas personuppgiftsbehandling som kan fungera som komplement till – eller, vid behov, genomföra delar av – den unionsrättsliga regleringen på området. Utredaren behöver i det sammanhanget också bedöma vilket utrymme förordningen ger för att i nationell rätt göra undantag från förordningens bestämmelser för myndigheternas personuppgiftsbehandling. Om utredaren bedömer att det finns förutsättningar att skapa en sådan samlad reglering bör utredaren lämna de författningsförslag som han anser vara motiverade.

Utredningens uppdrag ändras därför på så sätt att uppdraget att analysera registerförfattningar inom tre olika verksamhetsområden och lämna förslag på registerförfattningar för dessa verksamheter utgår.

Mot bakgrund av att utredningens uppdrag att överväga vilka typer av allmänna handlingar som myndigheterna bör vara skyldiga att lämna ut i elektronisk form är knutet till de tre verksamhetsområden som skulle analyseras närmare, är det med den ändrade inriktningen av uppdraget inte längre ändamålsenligt att inom ramen för denna utredning utreda utlämnandefrågan vidare. Utredningens uppdrag ändras därför på så sätt att även uppdraget att överväga frågan om skyldigheten att lämna ut allmänna handlingar i elektronisk form utgår.

Utredningen ska överväga hur en generell reglering bör utformas utifrån vad som är lämpligt från bl.a. normgivningstekniska och systematiska utgångspunkter.

Som framgår ovan omfattas personuppgiftsbehandling inom den brottsbekämpande verksamheten inte av kommissionens förslag till en allmän uppgiftsskyddsförordning utan av ett förslag till ett direktiv. Personuppgiftsbehandling inom den sektorn ska mot bakgrund av detta undantas från utredningens arbete och omfattas inte av det nu preciserade uppdraget. Vid utformningen av en ny reglering behöver utredaren dock ta hänsyn till hur regleringen på såväl detta som andra områden är utformad för att regelverken inte ska komma i konflikt med varandra. Den generella regleringen bör om möjligt vara utformad så att den kan tillämpas på ett enhetligt sätt av

myndigheter vars verksamhet i vissa delar kommer att omfattas av tillämpningsområdet för EU-förordningen och i andra delar omfattas av tillämpningsområdet för EU-direktivet.

Utredningen ska i sitt arbete noga följa den fortsatta behandlingen inom EU av förslaget till reformerad dataskyddsreglering. De förslag till författningsreglering som utredningen lämnar ska vara väl anpassade till denna översyn och dess resultat.

I övrigt gäller uppdraget oförändrat såsom det har redovisats i de ursprungliga direktiven.

Förlängd tid för uppdraget

Utredningstiden förlängs. Uppdraget ska redovisas senast den 30 januari 2015.

(Justitiedepartementet)

Kommittédirektiv 2014:147

Tilläggsdirektiv till informationshanteringsutredningen (Ju 2011:11)

Beslut vid regeringssammanträde den 20 november 2014

Förlängd tid för uppdraget

Regeringen beslutade den 6 oktober 2011 kommittédirektiv om integritet, effektivitet och öppenhet i en modern e-förvaltning (dir. 2011:86). Enligt utredningens direktiv skulle uppdraget redovisas senast den 1 december 2014. I tilläggsdirektiv beslutade regeringen den 6 mars 2014 bl.a. att förlänga utredningstiden till den 30 januari 2015 (dir. 2014:31).

Utredningstiden förlängs på nytt. Uppdraget ska i stället redovisas senast den 31 mars 2015.

(Justitiedepartementet)

Statens offentliga utredningar 2015

Kronologisk förteckning

1. Deltagande med väpnad styrka i utbildning utomlands. En utökad beslutsbefogenhet för regeringen. Fö.
2. Värdepappersmarknaden MiFID II och MiFIR. + Bilagor. Fi.
3. Med fokus på kärnuppgifterna. En angelägen anpassning av Polismyndighetens uppgifter på djurområdet. Ju.
4. Ett svenskt tonnageskattesystem. Fi.
5. En ny svensk tullagstiftning. Fi.
6. Mer gemensamma tobaksregler. Ett genomförande av tobaksproduktdirektivet. S.
7. Krav på privata aktörer i välfärden. Fi.
8. En översyn av årsredovisningslagarna. Ju.
9. En modern reglering av järnvägstransporter. Ju.
10. Gränser i havet. UD.
11. Kunskapsläget på kärnavfallsområdet 2015. Kontroll, dokumentation och finansiering för ökad säkerhet. M.
12. Överprövning av upphandlingsmål m.m. Fi.
13. Tillämpningsdirektivet till utstationeringsdirektivet – Del I. A.
14. Sedd, hörd och respekterad. Ett ändamålsenligt klagomålssystem i hälso- och sjukvården. S.
15. Attraktiv, innovativ och hållbar – strategi för en konkurrenskraftig jordbruks- och trädgårdsnäring. N L.
16. Ökat värdeskapande ur immateriella tillgångar. N.
17. För kvalitet – Med gemensamt ansvar. S.
18. Lösöreköp och registerpant. Ju.
19. En ny ordning för redovisningstillsyn. Fi.
20. Trygg och effektiv utskrivning från sluten vård. S.
21. Mer trygghet och bättre försäkring. Del 1 + 2. S.
22. Rektorn och styrkedjan. U.
23. Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten. Ju Fö.
24. En kommunallag för framtiden. Del A + B . Fi.
25. En ny säkerhetsskyddslag. Ju.
26. Begravningsclearing. Ku.
27. Skatt på dubbdäcksanvändning i tätort? Fi.
28. Gör Sverige i framtiden – digital kompetens. N.
29. En yrkesinriktning inom teknikprogrammet. U.
30. Kemikalieskatt. Skatt på vissa konsumentvaror som innehåller kemikalier. Fi.
31. Datalagring och integritet. Ju.
32. Nästa fas i e-hälsoarbetet. S.
33. Uppgiftslämnarservice för företagen. N.
34. Ett effektivare främjandeförbud i lotterilagen. Fi.
35. Service i glesbygd. N.
36. Systematiska jämförelser. För lärande i staten. S.
37. Översyn av lagen om skiljeförfarande. Ju.
38. Tillämpningsdirektivet till utstationeringsdirektivet – Del II. A.
39. Myndighetsdatalag. Ju.

Statens offentliga utredningar 2015

Systematisk förteckning

Utbildningsdepartementet

Utrikesdepartementet