Lagrådsremiss

Ny dataskyddslag

Regeringen överlämnar denna remiss till Lagrådet.

Stockholm den 21 december 2017

Morgan Johansson

David Törngren
(Justitiedepartementet)

Lagrådsremissens huvudsakliga innehåll

Regeringen föreslår att personuppgiftslagen upphävs och att en ny lag med kompletterande bestämmelser till EU:s dataskyddsförordning införs. Vidare föreslås att vissa bestämmelser i offentlighets- och sekretesslagen ändras.

Den föreslagna lagen innehåller bl.a. bestämmelser om att dataskyddsförordningen med vissa undantag ska gälla även utanför sitt egentliga tillämpningsområde, t.ex. i verksamhet som rör nationell säkerhet. Lagen ska dock vara subsidiär i förhållande till annan lag eller förordning, vilket möjliggör avvikande bestämmelser i s.k. registerförfattningar. Lagförslaget förtydligar under vilka förutsättningar personuppgifter får behandlas med stöd av dataskyddsförordningen. Regeringen föreslår bl.a. att ett barn som är minst 13 år ska kunna samtycka till behandling av personuppgifter i samband med användning av informationssamhällets tjänster, t.ex. sociala medier. Vidare föreslås att sanktionsavgifter ska kunna tas ut även då en myndighet bryter mot dataskyddsförordningen. Förslaget till ny lag innehåller också vissa bestämmelser om begränsning av de registrerades rättigheter samt om skadestånd och överklagande av bl.a. tillsynsmyndighetens beslut.

Slutligen anges att dataskyddsförordningen och den nya lagen inte ska tillämpas i den utsträckning det strider mot tryckfrihetsförordningen eller yttrandefrihetsgrundlagen.

Lagändringarna föreslås träda i kraft den 25 maj 2018.

Innehållsförteckning

1 Beslut

Regeringen har beslutat att inhämta Lagrådets yttrande över förslag till

1. lag med kompletterande bestämmelser till EU:s dataskyddsförordning,
2. lag om ändring i offentlighets- och sekretesslagen (2009:400).

2 Lagtext

Regeringen har följande förslag till lagtext.

2.1 Förslag till lag med kompletterande bestämmelser till EU:s dataskyddsförordning

Härigenom föreskrivs följande.

1 kap. Inledande bestämmelser

1 § Denna lag kompletterar Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), här benämnd EU:s dataskyddsförordning.

Termer och uttryck i denna lag har samma betydelse som i EU:s dataskyddsförordning. Med känsliga personuppgifter avses i denna lag sådana uppgifter som avses i artikel 9.1 i EU:s dataskyddsförordning.

Tillämpningsområde

2 § EU:s dataskyddsförordning, i den ursprungliga lydelsen, ska i tillämpliga delar gälla även vid behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av unionsrätten och i verksamhet som omfattas av avdelning V kapitel 2 i fördraget om Europeiska unionen. Denna lag kompletterar EU:s dataskyddsförordning även vid sådan behandling.

3 § Bestämmelserna i 2 § gäller inte i verksamhet som omfattas av

1. lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst,
2. lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet, eller
3. 6 kap. polisdatalagen (2010:361).

4 § Artiklarna 33 och 34 i EU:s dataskyddsförordning tillämpas inte i fråga om personuppgiftsincidenter som ska rapporteras enligt säkerhetsskyddslagen (1996:627) eller föreskrifter som har meddelats i anslutning till den lagen.

5 § Denna lag gäller vid behandling av personuppgifter som utförs av personuppgiftsansvariga eller personuppgiftsbiträden som är etablerade i Sverige, om behandlingen utförs inom ramen för verksamhet som bedrivs vid verksamhetsställen här i landet. Lagen gäller även vid behandling av personuppgifter som utförs av personuppgiftsansvariga som är etablerade på en annan plats där svensk rätt gäller enligt folkrätten.

Lagen gäller också vid behandling av personuppgifter som utförs av personuppgiftsansvariga eller personuppgiftsbiträden som endast är etablerade i tredjeland, om behandlingen avser registrerade som befinner sig i Sverige och har anknytning till

1. utbjudande av varor eller tjänster till sådana registrerade, eller
2. övervakning av deras beteende i Sverige.

Bestämmelsen i 2 kap. 1 § gäller vid behandling av personuppgifter som avser barn som bor i Sverige, oavsett var de personuppgiftsansvariga eller personuppgiftsbiträdena är etablerade.

Avvikande bestämmelser i annan författning

6 § Om en annan lag eller en förordning innehåller någon bestämmelse som avviker från denna lag, tillämpas den bestämmelsen.

Förhållandet till tryck- och yttrandefriheten

7 § EU:s dataskyddsförordning och denna lag ska inte tillämpas i den utsträckning det skulle strida mot tryckfrihetsförordningen eller yttrandefrihetsgrundlagen.

Artiklarna 5–30 och 35–50 i EU:s dataskyddsförordning samt 2–5 kap. denna lag ska inte tillämpas på behandling av personuppgifter som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande.

Tystnadsplikt för dataskyddsombud

8 § Den som fullgör uppgift som dataskyddsombud enligt artikel 37 i EU:s dataskyddsförordning får inte obehörigen röja det som han eller hon vid fullgörandet av sin uppgift har fått kännedom om.

I det allmännas verksamhet tillämpas offentlighets- och sekretesslagen (2009:400) i stället för första stycket.

2 kap. Rättslig grund för behandling av personuppgifter

Barns samtycke

1 § Vid erbjudande av informationssamhällets tjänster direkt till ett barn som bor i Sverige ska behandling av personuppgifter vara tillåten med stöd av barnets samtycke, om barnet är minst 13 år. Om barnet är under 13 år, ska sådan behandling vara tillåten endast om samtycke ges eller godkänns av den person som har föräldraansvar för barnet.

Rättslig förpliktelse

2 § Personuppgifter får behandlas med stöd av artikel 6.1 c i EU:s dataskyddsförordning, om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna fullgöra en rättslig förpliktelse som följer av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning.

Uppgift av allmänt intresse och myndighetsutövning

3 § Personuppgifter får behandlas med stöd av artikel 6.1 e i EU:s dataskyddsförordning, om behandlingen är nödvändig

1. för att utföra en uppgift av allmänt intresse som följer av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning, eller

2. som ett led i den personuppgiftsansvariges myndighetsutövning enligt lag eller annan författning.

Enskilda arkiv

4 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om att personuppgiftsansvariga som inte omfattas av föreskrifter om arkiv får behandla personuppgifter för arkivändamål av allmänt intresse.

Den myndighet som regeringen bestämmer får även i enskilda fall besluta att sådana personuppgiftsansvariga får behandla personuppgifter för arkivändamål av allmänt intresse. Ett beslut får förenas med villkor.

3 kap. Vissa kategorier av personuppgifter

Känsliga personuppgifter

Arbetsrätt, social trygghet och socialt skydd

1 § Känsliga personuppgifter får behandlas med stöd av artikel 9.2 b i EU:s dataskyddsförordning, om behandlingen är nödvändig för att den personuppgiftsansvarige eller den registrerade ska kunna fullgöra sina skyldigheter och utöva sina särskilda rättigheter inom arbetsrätten och inom områdena social trygghet och socialt skydd.

Personuppgifter som behandlas med stöd av första stycket får lämnas ut till tredje part endast om det inom arbetsrätten eller inom områdena social trygghet och socialt skydd finns en skyldighet för den personuppgiftsansvarige att göra det eller om den registrerade uttryckligen har samtyckt till utlämnandet.

Viktigt allmänt intresse

2 § Känsliga personuppgifter får behandlas av en myndighet med stöd av artikel 9.2 g i EU:s dataskyddsförordning

1. om uppgifterna har lämnats till myndigheten och behandlingen krävs enligt lag,

2. om behandlingen är nödvändig för handläggningen av ett ärende, eller

3. i enstaka fall, om behandlingen är nödvändig med hänsyn till ett viktigt allmänt intresse och inte innebär ett otillbörligt intrång i den registrerades personliga integritet.

Vid tillämpningen av första stycket 1 ska andra än myndigheter jämställas med myndigheter, i den utsträckning bestämmelserna om allmänna handlingar och sekretess i tryckfrihetsförordningen och offentlighets- och sekretesslagen (2009:400) gäller i deras verksamhet.

3 § Vid behandling som sker enbart med stöd av 2 § är det förbjudet att utföra sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter.

4 § Regeringen får meddela ytterligare föreskrifter om sådan behandling av känsliga personuppgifter som är nödvändig med hänsyn till ett viktigt allmänt intresse.

Hälso- och sjukvård och social omsorg

5 § Känsliga personuppgifter får behandlas med stöd av artikel 9.2 h i EU:s dataskyddsförordning, om behandlingen är nödvändig för

1. förebyggande hälso- och sjukvård och yrkesmedicin,
2. bedömningen av en arbetstagares arbetskapacitet,
3. medicinska diagnoser,
4. tillhandahållande av hälso- och sjukvård eller behandling,
5. social omsorg, eller
6. förvaltning av social omsorg, hälso- och sjukvårdstjänster samt deras system.

Behandling enligt första stycket får ske under förutsättning att kravet på tystnadsplikt i artikel 9.3 i EU:s dataskyddsförordning är uppfyllt.

Arkiv

6 § Känsliga personuppgifter får behandlas för arkivändamål av allmänt intresse med stöd av artikel 9.2 j i EU:s dataskyddsförordning, om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna följa föreskrifter om arkiv.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om att personuppgiftsansvariga som inte omfattas av föreskrifter om arkiv får behandla känsliga personuppgifter för arkivändamål av allmänt intresse.

Den myndighet som regeringen bestämmer får även i enskilda fall besluta att sådana personuppgiftsansvariga får behandla känsliga personuppgifter för arkivändamål av allmänt intresse. Ett beslut får förenas med villkor.

Statistik

7 § Känsliga personuppgifter får behandlas med stöd av artikel 9.2 j i EU:s dataskyddsförordning, om behandlingen är nödvändig för statistiska ändamål och samhällsintresset av det statistikprojekt där behandlingen ingår klart väger över den risk för otillbörligt intrång i enskildas personliga integritet som behandlingen kan innebära.

Personuppgifter som rör lagöverträdelser

8 § Personuppgifter som avses i artikel 10 i EU:s dataskyddsförordning får behandlas av myndigheter.

Även andra än myndigheter får behandla sådana personuppgifter, om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna följa föreskrifter om arkiv.

9 § Regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om i vilka fall andra än myndigheter får behandla sådana personuppgifter som avses i artikel 10 i EU:s dataskyddsförordning.

Den myndighet som regeringen bestämmer får även i enskilda fall besluta att andra än myndigheter får behandla sådana uppgifter. Ett beslut får förenas med villkor.

Personnummer och samordningsnummer

10 § Personnummer och samordningsnummer får behandlas utan samtycke endast när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl.

11 § Regeringen får meddela ytterligare föreskrifter om i vilka fall behandling av personnummer och samordningsnummer är tillåten.

4 kap. Användningsbegränsningar

Arkiv

1 § Personuppgifter som behandlas enbart för arkivändamål av allmänt intresse får användas för att vidta åtgärder i fråga om den registrerade endast om det finns synnerliga skäl med hänsyn till den registrerades vitala intressen.

Första stycket hindrar inte myndigheter från att använda personuppgifter som finns i allmänna handlingar.

Vid tillämpningen av andra stycket ska andra än myndigheter jämställas med myndigheter, i den utsträckning bestämmelserna om allmänna handlingar och sekretess i tryckfrihetsförordningen och offentlighets- och sekretesslagen (2009:400) gäller i deras verksamhet.

Statistik

2 § Personuppgifter som behandlas enbart för statistiska ändamål får användas för att vidta åtgärder i fråga om den registrerade endast om det finns synnerliga skäl med hänsyn till den registrerades vitala intressen.

5 kap. Begränsningar av vissa rättigheter och skyldigheter

Information och tillgång till personuppgifter

1 § Artiklarna 13–15 i EU:s dataskyddsförordning om information och tillgång till personuppgifter gäller inte sådana uppgifter som den personuppgiftsansvarige inte får lämna ut till den registrerade enligt lag eller annan författning eller enligt beslut som har meddelats med stöd av författning.

Om den personuppgiftsansvarige inte är en myndighet, gäller undantaget i första stycket även för uppgifter som hos en myndighet skulle ha varit sekretessbelagda enligt offentlighets- och sekretesslagen (2009:400).

2 § Artikel 15 i EU:s dataskyddsförordning om den registrerades rätt till tillgång gäller inte personuppgifter i löpande text som inte har fått sin slutliga utformning när begäran gjordes eller som utgör minnesanteckning eller liknande.

Undantaget i första stycket gäller inte om personuppgifterna

1. har lämnats ut till tredje part,
2. behandlas enbart för arkivändamål av allmänt intresse eller statistiska ändamål, eller
3. har behandlats under längre tid än ett år i löpande text som inte har fått sin slutliga utformning.

Bemyndigande

3 § Regeringen får meddela ytterligare föreskrifter om begränsningar enligt artiklarna 23, 89.2 och 89.3 i EU:s dataskyddsförordning.

6 kap. Tillsynsmyndighetens handläggning och beslut

Befogenheter

1 § De befogenheter som tillsynsmyndigheten har enligt artikel 58.1, 58.2 och 58.3 i EU:s dataskyddsförordning gäller vid tillsyn över att bestämmelserna i denna lag och andra föreskrifter som kompletterar EU:s dataskyddsförordning följs.

Första stycket innebär inte att tillsynsmyndigheten får ta ut sanktionsavgifter vid andra överträdelser än de som avses i artikel 83 i EU:s dataskyddsförordning.

Ansökan hos allmän förvaltningsdomstol

2 § Om tillsynsmyndigheten anser att det finns synnerliga skäl, får den ansöka hos allmän förvaltningsdomstol om att en åtgärd enligt artikel 58.2 i EU:s dataskyddsförordning ska vidtas, i stället för att själv besluta om åtgärden.

Ansökan ska göras hos den förvaltningsrätt som är behörig att pröva ett överklagande av tillsynsmyndighetens beslut.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Sanktionsavgifter

3 § Tillsynsmyndigheten får ta ut en sanktionsavgift av en myndighet vid överträdelser som avses i artikel 83.4, 83.5 och 83.6 i EU:s dataskyddsförordning, i den ursprungliga lydelsen. Då ska artikel 83.1, 83.2 och 83.3 i förordningen tillämpas.

Sanktionsavgiften ska bestämmas till högst 5 000 000 kronor vid överträdelser som avses i artikel 83.4 i EU:s dataskyddsförordning och till högst 10 000 000 kronor vid överträdelser som avses i artikel 83.5 och 83.6 i förordningen.

4 § Tillsynsmyndigheten får ta ut en sanktionsavgift vid överträdelser av artikel 10 i EU:s dataskyddsförordning, i den ursprungliga lydelsen. Då

ska artikel 83.1, 83.2 och 83.3 i förordningen tillämpas. Avgiftens storlek ska bestämmas med tillämpning av artikel 83.5 i förordningen.

5 § En sanktionsavgift får inte beslutas, om den som avgiften ska tas ut av inte har fått tillfälle att yttra sig inom fem år från den dag då överträdelsen ägde rum.

Ett beslut om sanktionsavgift ska delges.

6 § En sanktionsavgift tillfaller staten.

7 § En sanktionsavgift ska betalas till den myndighet som regeringen bestämmer inom 30 dagar från det att beslutet om att ta ut avgiften har fått laga kraft eller inom den längre tid som anges i beslutet.

Om sanktionsavgiften inte betalas inom den tid som anges i första stycket, ska myndigheten lämna den obetalda avgiften för indrivning. Bestämmelser om indrivning finns i lagen (1993:891) om indrivning av statliga fordringar m.m. Vid indrivning får verkställighet ske enligt utsökningsbalken.

8 § Regeringen får meddela ytterligare föreskrifter om sanktionsavgifter enligt EU:s dataskyddsförordning och denna lag.

7 kap. Skadestånd och överklagande

Skadestånd

1 § Rätten till ersättning från den personuppgiftsansvarige eller personuppgiftsbiträdet enligt artikel 82 i EU:s dataskyddsförordning gäller vid överträdelser av bestämmelser i denna lag och andra föreskrifter som kompletterar EU:s dataskyddsförordning.

Överklagande av personuppgiftsansvariga myndigheters beslut

2 § Beslut enligt artiklarna 12.5 och 15–21 i EU:s dataskyddsförordning som har meddelats av en myndighet i egenskap av personuppgiftsansvarig får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

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

Överklagande av tillsynsmyndighetens beslut

3 § Tillsynsmyndighetens beslut enligt EU:s dataskyddsförordning och enligt 6 kap. 3 och 4 §§ denna lag får överklagas till allmän förvaltningsdomstol. När ett beslut överklagas, är tillsynsmyndigheten motpart i domstolen.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Överklagande av andra beslut

4 § Beslut enligt 2 kap. 4 § andra stycket, 3 kap. 6 § tredje stycket och 3 kap. 9 § andra stycket denna lag får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Överklagandeförbud

5 § Andra beslut enligt EU:s dataskyddsförordning eller denna lag än de som avses i 2–4 §§ och 6 kap. 2 § får inte överklagas.

---

1. Denna lag träder i kraft den 25 maj 2018.
2. Genom lagen upphävs personuppgiftslagen (1998:204).
3. I stället för vad som sägs i 1 kap. 2 §, ska den upphävda lagen fortsätta att gälla i sådan verksamhet hos Försvarsmakten, Försvarets radioanstalt och Totalförsvarets rekryteringsmyndighet som inte omfattas av unionsrätten.
4. Den upphävda lagen gäller fortfarande vid sådan behandling av personuppgifter som avses i artikel 2.2 d i EU:s dataskyddsförordning, i den ursprungliga lydelsen.
5. Den upphävda lagen gäller fortfarande i den utsträckning som det i en annan lag eller en förordning finns bestämmelser som innehåller hänvisningar till den lagen.
6. Den upphävda lagen gäller fortfarande för överklagande av beslut som har meddelats med stöd av den lagen.
7. Bestämmelsen i 49 § den upphävda lagen gäller fortfarande för överträdelser som har skett före ikraftträdandet.
8. Beslut som har meddelats med stöd av 21 § fjärde stycket den upphävda lagen gäller fortfarande.

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

Härigenom föreskrivs att 10 kap. 27 § och 21 kap. 7 § och rubriken närmast före 21 kap. 7 § offentlighets- och sekretesslagen (2009:400) ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
10 kap.	
27 §[1]	
Utöver vad som följer av 2, 3, 5 och 15–26 §§ 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.	
Första stycket gäller inte i fråga om sekretess enligt 24 kap. 2 a och 8 §§, 25 kap. 1–8 §§, 26 kap. 1–6 §§, 29 kap. 1 och 2 §§, 31 kap. 1 § första stycket, 2 och 12 §§, 33 kap. 2 §, 36 kap. 3 § samt 40 kap. 2 och 5 §§.	
Första stycket gäller inte heller om utlämnandet strider mot lag eller förordning *eller föreskrift som har meddelats med stöd av personuppgiftslagen (1998:204)*.	Första stycket gäller inte heller om utlämnandet strider mot lag eller förordning.
21 kap.	
Behandling i strid med *personuppgiftslagen*	Behandling i strid med *dataskyddsregleringen*
7 §	
Sekretess gäller för personuppgift, om det kan antas att ett utlämnande *skulle medföra att uppgiften* behandlas i strid med *personuppgiftslagen (1998:204)*.	Sekretess gäller för personuppgift, om det kan antas att *uppgiften efter* ett utlämnande *kommer att* behandlas i strid med *Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), i den ursprungliga lydelsen, eller lagen (2018:00) med kompletterande bestämmelser till EU:s dataskyddsförordning.*

Denna lag träder i kraft den 25 maj 2018.

[1] Senaste lydelse 2013:795.

3 Ärendet och dess beredning

Den 27 april 2016 utfärdades Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), nedan kallad dataskyddsförordningen. Dataskyddsförordningen, som börjar tillämpas den 25 maj 2018, finns i svensk lydelse i *bilaga 1*.

Den 25 februari 2016 beslutade regeringen att ge en särskild utredare i uppdrag att föreslå de anpassningar och kompletterande författningsbestämmelser på generell nivå som dataskyddsförordningen ger anledning till (dir. 2016:15). Utredningen, som tog namnet Dataskyddsutredningen (Ju 2016:04), överlämnade den 12 maj 2017 betänkandet Ny dataskyddslag – Kompletterande bestämmelser till EU:s dataskyddsförordning (SOU 2017:39). En sammanfattning av betänkandet finns i *bilaga 2*. Betänkandets lagförslag finns i *bilaga 3*.

Betänkandet har remissbehandlats. En förteckning över remissinstanserna finns i *bilaga 4*. Remissvaren finns tillgängliga i Justitiedepartementet (Ju2017/04264/L6).

Justitiedepartementet har i en promemoria som kompletterar betänkandet lämnat förslag avseende den nya lagens territoriella tillämpningsområde. En sammanfattning av promemorian finns i *bilaga 5*. Promemorians lagförslag finns i *bilaga 6.* Promemorian har remissbehandlats. En förteckning över remissinstanserna finns i *bilaga 7*. Remissvaren finns tillgängliga i Justitiedepartementet (Ju2017/06940/L6).

Förslag till undantag från bestämmelsen som utsträcker dataskyddsförordningens tillämpningsområde har beretts med Säkerhetspolisen, Datainspektionen, Säkerhets- och integritetsskyddsnämnden, Myndigheten för samhällsskydd och beredskap, Försvarsmakten, Försvarets radioanstalt och Totalförsvarets rekryteringsmyndighet. Myndigheternas svar finns tillgängliga i Justitiedepartementet (Ju2017/04264/L6).

Vissa frågor av övergångskaraktär behandlas i Utredningen om 2016 års dataskyddsdirektivs delbetänkande Brottsdatalag (SOU 2017:29, Ju2017/03283/L4).

4 EU:s dataskyddsreform

4.1 Gällande rätt

Den allmänna regleringen om behandling av personuppgifter inom EU finns i dag i 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 (dataskyddsdirektivet). Dataskyddsdirektivet gäller inte för behandling av personuppgifter på områden som faller utanför unionsrätten, t.ex. allmän säkerhet och försvar samt statens verksamhet på straffrättens område. Rådets rambeslut 2008/977/RIF av den 27 november 2008 om

skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete (dataskyddsrambeslutet) är tillämpligt på informationsutbyte över gränserna. Dataskyddsrambeslutet gäller däremot inte för rent nationell personuppgiftsbehandling inom exempelvis polisens område. Från dataskyddsrambeslutets tillämpningsområde undantas också personuppgiftsbehandling inom området nationell säkerhet. På detta område finns det således inte någon EU-gemensam reglering om behandling av personuppgifter.

Dataskyddsdirektivet har genomförts i svensk rätt huvudsakligen genom personuppgiftslagen (1998:204), förkortad PUL. Bestämmelserna i personuppgiftslagen har till syfte att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter. Personuppgiftslagen följer i princip dataskyddsdirektivets struktur och innehåller liksom direktivet bestämmelser om bl.a. personuppgiftsansvar, grundläggande krav för behandling av personuppgifter och information till den registrerade.

Personuppgiftslagen är tillämplig även utanför EU-rättens område och gäller både för myndigheter och enskilda som behandlar personuppgifter. Personuppgiftslagen är samtidigt subsidiär, vilket innebär att lagens bestämmelser inte ska tillämpas om det finns avvikande bestämmelser i en annan lag eller en förordning. Det finns en stor mängd sådana bestämmelser i sektorsspecifika författningar som främst reglerar hur olika myndigheter får behandla personuppgifter.

Personuppgiftslagen kompletteras också av bestämmelser i personuppgiftsförordningen (1998:1191), förkortad PUF, som bl.a. pekar ut Datainspektionen som tillsynsmyndighet. Datainspektionen bemyndigas i förordningen att meddela närmare föreskrifter om bl.a. i vilka fall behandling av personuppgifter är tillåten och vilka krav som ställs på den personuppgiftsansvarige.

4.2 En ny förordning och ett nytt direktiv

Europeiska kommissionen lade fram sitt förslag till en reformerad dataskyddsreglering i EU år 2012. Förslaget bestod av dels en förordning med allmänna regler om skydd av personuppgifter som skulle ersätta dataskyddsdirektivet, dels ett direktiv med regler om skydd av personuppgifter som behandlas i samband med förebyggande, utredning, avslöjande eller lagföring av brott och därmed förbunden rättslig verksamhet som skulle ersätta dataskyddsrambeslutet.

Den 27 april 2016 antogs dataskyddsförordningen. Samma dag antogs Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF, nedan kallat det nya dataskyddsdirektivet.

Dataskyddsförordningen kommer från och med den 25 maj 2018 att ersätta dataskyddsdirektivet och utgöra den generella regleringen av personuppgiftsbehandling inom EU. Enligt artikel 288 andra stycket i

fördraget om Europeiska unionens funktionssätt ska en EU-förordning ha allmän giltighet och vara till alla delar bindande och direkt tillämplig i varje medlemsstat. Trots att dataskyddsförordningen, till skillnad från dataskyddsdirektivet, är direkt tillämplig innehåller den många bestämmelser som förutsätter eller ger utrymme för kompletterande nationella bestämmelser av olika slag. Förordningen har därmed i vissa delar en direktivliknande karaktär. I skäl 8 till förordningen anges också att om förordningen föreskriver förtydliganden eller begränsningar av dess bestämmelser genom medlemsstaternas nationella rätt kan medlemsstaterna, i den utsträckning det är nödvändigt för samstämmigheten och för att göra de nationella bestämmelserna begripliga för de personer som de tillämpas på, införliva delar av förordningen i nationell rätt.

4.3 Förordningens syfte

I skäl 9 till förordningen konstateras att dataskyddsdirektivet inte har kunnat förhindra bristande enhetlighet i genomförandet och tillämpningen av dataskyddet i olika delar av unionen. Skillnader i nivån på skyddet av personuppgifter kan enligt skälet förhindra det fria flödet av personuppgifter och kan därför utgöra ett hinder för att bedriva ekonomisk verksamhet på unionsnivå, snedvrida konkurrensen och hindra myndigheterna från att fullgöra sina skyldigheter enligt unionsrätten.

För att säkerställa en enhetlig skyddsnivå över hela unionen och undvika avvikelser som hindrar den fria rörligheten av personuppgifter inom den inre marknaden behövs, enligt skäl 13 till förordningen, en förordning som skapar rättslig säkerhet och öppenhet för ekonomiska aktörer och som ger fysiska personer i alla medlemsstater samma rättsligt verkställbara rättigheter och skyldigheter samt ålägger personuppgiftsansvariga och personuppgiftsbiträden samma ansvar. På så sätt blir övervakningen av behandling av personuppgifter enhetlig, sanktionerna i alla medlemsstater likvärdiga och samarbetet mellan tillsynsmyndigheterna i olika medlemsstater effektivt.

4.4 Tillämpningsområdet

Dataskyddsförordningen ska, precis som dataskyddsdirektivet, tillämpas på sådan behandling av personuppgifter som helt eller delvis företas på automatisk väg samt på annan behandling än automatisk av personuppgifter som ingår i eller kommer att ingå i ett register.

Från dataskyddsförordningens tillämpningsområde undantas behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av unionsrätten eller som utförs av medlemsstaterna när de bedriver verksamhet som omfattas av den gemensamma utrikes- och säkerhetspolitiken. Behandling av personuppgifter som utförs av en fysisk person som ett led i verksamhet av privat natur eller som har samband med hans eller hennes hushåll omfattas inte heller av förordningens bestämmelser. Vidare gäller förordningen inte för sådan behandling av personuppgifter som utförs av behöriga myndigheter för ända-

målen att förebygga, utreda, upptäcka eller lagföra brott eller verkställa straffrättsliga påföljder. Sådan behandling regleras i stället genom det nya dataskyddsdirektivet. Slutligen ska förordningens bestämmelser inte tillämpas av EU:s institutioner, organ och byråer. Den behandling av personuppgifter som sker där regleras i stället genom Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter. Ett förslag till reviderad förordning om skydd för personuppgifter som behandlas av unionens institutioner, organ, kontor och byråer har lagts fram av kommissionen (COM(2017) 8 final).

Dataskyddsförordningen ska tillämpas på all behandling av personuppgifter som sker inom ramen för den verksamhet som bedrivs av personuppgiftsansvariga eller personuppgiftsbiträden som är etablerade i unionen, oavsett om behandlingen utförs i unionen eller inte. En skillnad jämfört med dataskyddsdirektivet är att förordningen under vissa omständigheter ska tillämpas även på behandling av personuppgifter som utförs av personuppgiftsansvariga eller personuppgiftsbiträden som inte är etablerade i unionen. Detta gäller om behandlingen avser registrerade som befinner sig i unionen, under förutsättning att behandlingen har anknytning till antingen utbjudande av varor eller tjänster till sådana registrerade i unionen eller övervakning av deras beteende, så länge beteendet sker inom unionen. Slutligen ska dataskyddsförordningen också tillämpas på behandling av personuppgifter som utförs av en personuppgiftsansvarig som inte är etablerad i unionen, men på en plats där en medlemsstats nationella rätt gäller enligt folkrätten.

4.5 Sakliga förändringar

Dataskyddsförordningen baseras till stor del på dataskyddsdirektivets struktur och innehåll, men innebär även en rad förändringar. Några av dessa förtjänar att nämnas särskilt.

Den registrerades rättigheter förstärks i syfte att ge den registrerade ökad kontroll över sina personuppgifter. Den information som ska tillhandahållas den registrerade preciseras och utvidgas och det anges uttryckligen att den personuppgiftsansvarige ska tillhandahålla informationen i en begriplig och lättillgänglig form. Förordningen innebär även en förstärkning av rätten för den registrerade att få åtkomst till sina personuppgifter i syfte att föra över dem till en annan leverantör av elektroniska tjänster, s.k. dataportabilitet. Vidare införs en tydligare rätt till radering (rätt att bli bortglömd).

När informationssamhällets tjänster erbjuds direkt till ett barn, krävs enligt dataskyddsförordningen att samtycke eller godkännande av barnets samtycke i vissa fall inhämtas av den som har föräldraansvar för barnet för att personuppgifter som rör barnet ska få behandlas. Barns särställning och särskilda utsatthet poängteras på flera ställen i förordningen.

Genom förordningen införs en skyldighet för den personuppgiftsansvarige att anmäla till tillsynsmyndigheten om det inträffar en så kallad personuppgiftsincident, dvs. en säkerhetsincident som oavsiktligt på-

verkar behandlingen av personuppgifter. Även den registrerade ska informeras om incidenten om den sannolikt leder till en hög risk för enskildas rättigheter och friheter.

Det införs krav på konsekvensanalyser om en viss behandling sannolikt kommer att leda till hög risk för enskildas rättigheter eller skyldigheter. Den allmänna anmälningsskyldigheten till tillsynsmyndigheten tas däremot bort. Vidare införs det tydligare regler för kommunikation med den registrerade och ansvar för dem som behandlar personuppgifter. Ett krav på inbyggt dataskydd och dataskydd som standard införs.

Genom förordningen införs ett nytt gemensamt system med sanktionsavgifter som ska tas ut vid överträdelser av förordningen. Även på andra sätt innebär förordningen ett ökat fokus på en enhetlig tillämpning av dataskyddsreglerna inom EU, t.ex. genom åtgärder som godkännande av uppförandekoder och certifiering. Det införs även en skyldighet för de nationella tillsynsmyndigheterna att samarbeta med varandra och en mekanism för enhetlighet när flera tillsynsmyndigheter är inblandade. Det införs samtidigt en ny princip om en enda kontaktpunkt, som ska underlätta för sådana personuppgiftsansvariga som är verksamma i flera medlemsstater, genom att de endast ska behöva vara i kontakt med en av de behöriga tillsynsmyndigheterna. Det införs även ett nytt unionsorgan, Europeiska dataskyddsstyrelsen, som får långtgående befogenheter att uttala sig om tolkningen av förordningen även i enskilda fall.

Utrymmet för att ge offentlighetsprincipen företräde framför dataskyddsregleringen blir tydligare, genom en uttrycklig och direkt tillämplig bestämmelse i artikel 86 i dataskyddsförordningen. Av bestämmelsen följer att personuppgifter i allmänna handlingar får lämnas ut i enlighet med nationell rätt, för att jämka samman allmänhetens rätt att få tillgång till handlingar med rätten till skydd för personuppgifter i enlighet med förordningen. Artikeln möjliggör alltså en tillämpning av bestämmelserna i tryckfrihetsförordningen, förkortad TF, om allmänhetens tillgång till handlingar när det gäller allmänna handlingar som innehåller personuppgifter.

5 Ett nytt svenskt regelverk om dataskydd

5.1 En ny lag införs och personuppgiftslagen upphävs

Regeringens förslag: Personuppgiftslagen upphävs och en ny lag med bestämmelser som kompletterar EU:s dataskyddsförordning på ett generellt plan införs.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna tillstyrker förslaget eller har inga synpunkter på det. Bland andra *Myndigheten för vård- och omsorgsanalys* och *Göteborgs universitet* påpekar, utan att invända mot utredningens förslag, att dataskyddsreformen medför att rättsområdet blir mer komplext. Några myndigheter, bl.a. *Pensionsmyndigheten* och *Lantmäteriet*, framhåller

behovet av en samlad översyn av registerförfattningarna. Ett par remissinstanser, bl.a. *Sveriges konsumenter* och *Stiftelsen för internetinfrastruktur*, ifrågasätter utredningens strävan att varken utvidga eller inskränka möjligheterna till behandling av personuppgifter, annat än då dataskyddsförordningen kräver en sådan förändring. Flera remissinstanser, bl.a. *Domstolsverket*, *Myndigheten för vård- och omsorgsanalys*, *Konkurrensverket* och *Riksidrottsförbundet*, efterlyser mer vägledning kring hur olika termer och begrepp i dataskyddsförordningen ska tolkas och tillämpas. Vidare tar flera remissinstanser, bl.a. *Arbetsförmedlingen*, Riksidrottsförbundet och *Tjänstemännens centralorganisation*, upp frågor som är specifika för deras verksamhet eller den reglering som styr den.

Skälen för regeringens förslag: Dataskyddsförordningen ersätter dataskyddsdirektivet, som har genomförts i svensk rätt huvudsakligen genom personuppgiftslagen, personuppgiftsförordningen och Datainspektionens föreskrifter. Dataskyddsförordningen ska däremot inte implementeras i svensk rätt, utan i stället tillämpas direkt av enskilda, myndigheter och domstolar. När dataskyddsförordningen börjar tillämpas kommer alltså den generella regleringen om behandling av personuppgifter att finnas i dataskyddsförordningen. Det svenska generella regelverket om dataskydd kan då inte längre finnas kvar, eftersom det skulle leda till en otillåten dubbelreglering. Personuppgiftslagen bör därför upphävas.

Den omständigheten att den nya generella unionsrättsakten om dataskydd är en förordning, och inte ett direktiv, innebär således omfattande begränsningar av möjligheten att införa eller behålla nationella bestämmelser om dataskydd. Dataskyddsförordningen både förutsätter och medger emellertid nationella bestämmelser som kompletterar eller föreskriver undantag från förordningens regler. I skäl 8 till förordningen anges att om förordningen föreskriver förtydliganden eller begränsningar av dess bestämmelser genom medlemsstaternas nationella rätt, kan medlemsstaterna, i den utsträckning det är nödvändigt för samstämmigheten och för att göra de nationella bestämmelserna begripliga för de personer som de tillämpas på, införliva delar av förordningen i nationell rätt.

Vissa av de kompletterande bestämmelser som behövs eller är lämpliga är av generell karaktär, i betydelsen att de rör hela samhället eller flertalet myndigheter och inte bara en viss sektor. Denna typ av generella bestämmelser bör samlas i en ny övergripande lag om dataskydd. För att betona att lagen inte är heltäckande, utan endast utgör ett komplement till dataskyddsförordningen, bör den i enlighet med utredningens förslag benämnas lagen med kompletterande bestämmelser till EU:s dataskyddsförordning. I det följande kallas den nya lagen för dataskyddslagen.

Vidare har förordningen, framför allt när det gäller den offentliga sektorn, en direktivliknande karaktär och tillåter att förordningens regler specificeras i nationell rätt. Detta följer bl.a. av artikel 6.2, där det anges att medlemsstaterna får behålla eller införa mer specifika bestämmelser för att anpassa tillämpningen av bestämmelserna i förordningen när det gäller behandling som sker enligt artikel 6.1 c (rättslig förpliktelse) och 6.1 e (uppgift av allmänt intresse och myndighetsutövning). Detta får ske genom att medlemsstaterna närmare fastställer specifika krav för

uppgiftsbehandlingen och andra åtgärder för att säkerställa en laglig och rättvis behandling. Av skäl 10 framgår att detta även gäller för behandlingen av känsliga personuppgifter. Av artikel 6.3 framgår vidare att, vid behandling enligt artikel 6.1 c och e, ska den rättsliga grunden fastställas i unionsrätten eller i nationell rätt. Där anges också att den rättsliga grunden kan innehålla särskilda bestämmelser för att anpassa tillämpningen av bestämmelserna i dataskyddsförordningen, bl.a. de allmänna villkor som ska gälla för den personuppgiftsansvariges behandling, vilken typ av uppgifter som ska behandlas, vilka registrerade som berörs, de enheter till vilka personuppgifterna får lämnas ut och för vilka ändamål, ändamålsbegränsningar, lagringstid samt typer av behandling och förfaranden för behandling, inbegripet åtgärder för att tillförsäkra en laglig och rättvis behandling. Detta innebär att det även fortsättningsvis finns ett utrymme för sådan sektorsspecifik särreglering om behandling av personuppgifter som finns i de svenska registerförfattningarna, t.ex. studiestödsdatalagen (2009:287) och domstolsdatalagen (2015:728). Anpassningen av sådana sektorsspecifika författningar behandlas dock inte i detta lagstiftningsärende.

Flera remissinstanser tar upp frågor som är specifika för deras verksamhet och den reglering som styr den. Sådana sektorsspecifika frågor omfattas dock inte av detta lagstiftningsärende. Flera remissinstanser efterlyser också mer vägledning kring hur dataskyddsförordningens bestämmelser ska tolkas och tillämpas, framför allt i fråga om tillämplig rättslig grund. I detta lagstiftningsärende behandlas dock inte frågor som rör tillämpningen av dataskyddsförordningens direkt tillämpliga bestämmelser, annat än i samband med resonemang kring behovet och lämpligheten av kompletterande lagstiftning på generell nivå. Regeringen kan också konstatera att det i många fall är svårt att ge mer vägledning än den utredningen ger i betänkandet. När det gäller de nya begrepp som introduceras genom dataskyddsreformen finns det ännu inte någon praxis eller annan rättskälla att luta sig mot.

Det bör dock understrykas att tillsynsmyndigheten, enligt artikel 57.1 b, har i uppgift att öka personuppgiftsansvarigas och personuppgiftsbiträdens medvetenhet om sina skyldigheter enligt dataskyddsförordningen. Av skäl 132 framgår att medvetandehöjande kampanjer från tillsynsmyndighetens sida bör innefatta särskilda åtgärder riktade dels till personuppgiftsansvariga och personuppgiftsbiträden, inbegripet mikroföretag samt små och medelstora företag, dels till fysiska personer, särskilt i utbildningssammanhang. Dessutom har tillsynsmyndigheten, enligt artikel 57.1 b, i uppgift att öka allmänhetens medvetenhet om och förståelse för risker, regler, skyddsåtgärder och rättigheter i fråga om behandling. Särskild uppmärksamhet ska ägnas åt insatser som riktar sig till barn. Vidare har regeringen gett Datainspektionen i uppdrag att förstärka sitt arbete med att underlätta näringslivets anpassning till dataskyddsförordningen, för att svenska företag inte ska tappa tempo i sitt digitaliseringsarbete och samtidigt upprätthålla ett gott integritetsskydd (N2016/07306/FÖF).

Bland andra *Myndigheten för vård- och omsorgsanalys* och *Göteborgs universitet* påpekar, utan att invända mot utredningens förslag, att dataskyddsreformen medför att rättsområdet blir mer komplext. Regeringen har förståelse för dessa synpunkter. Det förhållandet att personuppgifts-

lagen ersätts av den mer omfattande regleringen i dataskyddsförordningen och en kompletterande nationell reglering på generell nivå, innebär att regelverket kan uppfattas som mer komplext. Det bör dock framhållas att den ökade komplexiteten är en följd av att det nya EU-rättsliga regelverket är direkt tillämpligt och att detta förutsätter kompletterande nationell reglering. Samtidigt kan konstateras att för de allra flesta personuppgiftsansvariga kommer endast dataskyddsförordningen och dataskyddslagen att vara tillämpliga. För personuppgiftsansvariga som har verksamhet i flera medlemsstater finns dessutom stora fördelar med en dataskyddsreglering som är direkt tillämplig i hela EU. Vidare har tillsynsmyndigheten, som beskrivs ovan, redan enligt dataskyddsförordningen ett uppdrag att informera om regleringen.

Några myndigheter, bl.a. *Pensionsmyndigheten* och *Lantmäteriet*, framhåller behovet av en samlad översyn av registerförfattningarna. Ett par remissinstanser, bl.a. *Sveriges konsumenter* och *Stiftelsen för internetinfrastruktur*, ifrågasätter utredningens strävan att varken utvidga eller inskränka möjligheterna till behandling av personuppgifter, annat än då dataskyddsförordningen kräver en sådan förändring. Regeringen kan emellertid konstatera att den korta tid som står till buds för att anpassa den svenska dataskyddsregleringen till den nya EU-regleringen inte medger mer omfattande nationella reformer på detta område. Det utesluter inte att vissa sådana övergripande förändringar skulle kunna vara befogade och därför bli föremål för överväganden i ett annat sammanhang.

5.1.1 Termer och uttryck

Regeringens förslag: Termer och uttryck i dataskyddslagen ska ha samma betydelse som i EU:s dataskyddsförordning.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: I stort sett alla instanser tillstyrker förslaget eller har inga synpunkter på det. *Myndigheten för vård- och omsorgsanalys* anser dock att det inte är användarvänligt att definitionerna inte anges i lagen.

Skälen för regeringens förslag: Många av de termer och uttryck som används i dataskyddsförordningen definieras i artikel 4 i förordningen. Andra begrepp definieras visserligen inte, men är av unionsrättslig karaktär och kan inte ges en särskild betydelse i nationell rätt. Termer och uttryck som används i dataskyddslagen bör därför ha samma betydelse som i dataskyddsförordningen. Med anledning av *Myndigheten för vård- och omsorgsanalys* synpunkt att förordningens definitioner bör anges i lagen, bör framhållas att lagen endast utgör ett komplement till dataskyddsförordningen. Det stora flertalet av de regler som ska tillämpas finns i dataskyddsförordningen och ska tillämpas direkt av myndigheter, företag och andra personuppgiftsansvariga. Om förordningens definitioner infördes i dataskyddslagen skulle det kunna ge intrycket av att lagen är fristående från förordningen.

5.1.2 Hänvisningsteknik

Regeringens förslag: De hänvisningar till EU:s dataskyddsförordning som finns i dataskyddslagen ska, med undantag för bestämmelsen om behandling av personuppgifter utanför dataskyddsförordningens egentliga tillämpningsområde och bestämmelserna om sanktionsavgifter, vara dynamiska, dvs. avse förordningen i den vid varje tidpunkt gällande lydelsen.

Utredningens förslag överensstämmer delvis med regeringens. Utredningen föreslår dynamiska hänvisningar till dataskyddsförordningen även i bestämmelserna om sanktionsavgifter.

Remissinstanserna tillstyrker förslaget eller har inga synpunkter på det.

Skälen för regeringens förslag: Den föreslagna dataskyddslagen innehåller hänvisningar till bestämmelser i dataskyddsförordningen. Hänvisningar till EU-rättsakter kan göras antingen statiska eller dynamiska. En statisk hänvisning innebär att hänvisningen avser EU-rättsakten i en viss angiven lydelse. En dynamisk hänvisning innebär att hänvisningen avser EU-rättsakten i den vid varje tidpunkt gällande lydelsen.

Dataskyddsförordningen är direkt tillämplig. För att säkerställa att ändringar i dataskyddsförordningen får omedelbart genomslag är det lämpligt att hänvisningarna dit görs dynamiska. Detta hindrar emellertid inte att dataskyddslagen kan behöva ändras om dataskyddsförordningens innehåll ändras. De hänvisningar till dataskyddsförordningen som finns i dataskyddslagen bör med vissa undantag vara dynamiska, dvs. avse förordningen i dess vid varje tidpunkt gällande lydelse. Hänvisningarna kommer således att omfatta även eventuella framtida ändringar i dataskyddsförordningen.

Flera av hänvisningarna till dataskyddsförordningen i de bestämmelser som regeringen föreslår är av upplysande karaktär. Det gäller främst hänvisningarna i bestämmelserna om rättslig grund, känsliga personuppgifter och skadestånd. Dynamiska hänvisningar behövs i dessa fall för att undvika osäkerhet. Detsamma gäller för hänvisningarna till dataskyddsförordningen avseende betydelsen av de termer och uttryck som används i lagen. Terminologin som används i den nationella reglering som kompletterar EU-förordningen måste följa den begreppsutveckling som sker inom unionen, även vid en eventuell ändring av uttryckliga definitioner i dataskyddsförordningen.

Andra hänvisningar till dataskyddsförordningen finns i förslagen till bestämmelser som rör bl.a. vilka myndigheter som är behöriga att pröva olika frågor eller som har att vidta åtgärder enligt dataskyddsförordningen samt vilka förfarandebestämmelser som ska gälla när förordningen saknar bestämmelser eller hänvisar till att nationell rätt ska tillämpas. Förslaget till dataskyddslag innehåller också en bestämmelse om tystnadsplikt för den som fullgör uppgift som dataskyddsombud enligt dataskyddsförordningen.

Samtliga författningsförslag som nämns i föregående stycke avser bestämmelser av ett slag som måste finnas i svensk rätt för att Sverige ska uppfylla sina unionsrättsliga förpliktelser. Hänvisningarna till data-

skyddsförordningen i dessa bestämmelser bör enligt regeringens mening vara dynamiska. Den omständigheten att somliga förändringar i dataskyddsförordningen skulle kunna föranleda behov av justeringar av svensk rätt, t.ex. rörande vilken myndighet eller domstol som ska hantera en viss fråga, utgör inte skäl för att välja statiska hänvisningar i dessa paragrafer.

Vidare förekommer det i lagförslaget bestämmelser som föreskriver undantag från dataskyddsförordningens bestämmelser om de registrerades rättigheter och den personuppgiftsansvariges skyldigheter. Flera av dessa undantag är nära förknippade med den svenska grundlagsregleringen om tryck- och yttrandefrihet och rätt till tillgång till allmänna handlingar eller med behovet av skydd för rikets säkerhet. Med hänsyn till vikten av att dessa intressen upprätthålls, bör dessa undantag gälla även om dataskyddsförordningens lydelse skulle komma att ändras i något avseende. Regeringen föreslår även undantag som motiveras av behovet av en balans mellan det skydd som dataskyddsförordningen ger den registrerade och det skydd som annan lagstiftning ger den personuppgiftsansvariges verksamhet eller tredje parts personliga integritet, t.ex. i form av sekretess. Även i dessa bestämmelser behövs det dynamiska hänvisningar för att säkerställa att balansen består även vid en eventuell ändring av dataskyddsförordningen.

När det gäller regleringen om behandling av personuppgifter utanför dataskyddsförordningens egentliga tillämpningsområde, finns det dock skäl att välja en statisk hänvisningsteknik, innebärande att hänvisningen ska avse den ursprungliga lydelsen av dataskyddsförordningen. Skälen för detta ställningstagande utvecklas i avsnitt 6.1.1. Dataskyddsförordningen innebär vidare att det i svensk rätt får eller måste införas bestämmelser om sanktioner vid överträdelser av förordningen. I de bestämmelser som avser sådana sanktioner bör hänvisningarna till dataskyddsförordningen vara statiska, se avsnitt 16.2 och 16.3.3.

Denna lagrådsremiss innehåller även förslag till ändringar i offentlighets- och sekretesslagen (2009:400), förkortad OSL, som innebär att en hänvisning till dataskyddsförordningen ska införas i en bestämmelse. Frågan om hänvisningens karaktär i det fallet behandlas i avsnitt 15.3.

5.1.3 Avvikande bestämmelser i annan lag eller i förordning ska ha företräde

Regeringens förslag: Om en annan lag eller en förordning innehåller någon bestämmelse som avviker från denna lag, tillämpas den bestämmelsen.

Utredningens förslag överensstämmer i sak med regeringens. Utredningen föreslår dock en annan utformning av författningsbestämmelsen.

Remissinstanserna: Det stora flertalet tillstyrker förslaget eller har inga synpunkter på det. *Kungliga tekniska högskolan* anser dock att det av lagtexten bör framgå att även direkt tillämpliga EU-förordningar omfattas. *Sveriges advokatsamfund* anser att det bör framgå av bestäm-

melsen att bestämmelser som avviker från dataskyddslagen ska tillämpas såvida de inte är oförenliga med dataskyddsförordningen.

Skälen för regeringens förslag: Personuppgiftslagen är subsidiär på så sätt att om det i en annan lag eller i en förordning finns bestämmelser som avviker från lagen, ska de bestämmelserna gälla (2 § PUL). Frågan är om en sådan ordning bör gälla även i fråga om dataskyddslagen.

Dataskyddsförordningen ger i viss utsträckning utrymme för undantag eller kompletteringar avseende en särskild typ av verksamhet, se avsnitt 5.1. Dataskyddslagen kommer endast att innehålla övergripande och generella bestämmelser. De flesta bestämmelser som kompletterar förordningen kommer således att finnas i någon annan författning.

Dataskyddslagen är, i likhet med personuppgiftslagen, av offentligrättslig karaktär. Som helhet måste den även betraktas som betungande i förhållande till de personuppgiftsansvariga och personuppgiftsbiträden som träffas av den. Dataskyddslagens bestämmelser gäller inte bara för statliga myndigheter, utan även för kommuner, företag och enskilda. Det krävs därför enligt 8 kap. 2 § första stycket 2 och 3 § regeringsformen, förkortad RF, bemyndiganden i lag för att anslutande föreskrifter ska kunna meddelas av regeringen eller av en förvaltningsmyndighet.

När det däremot gäller sektorsspecifika författningar som enbart rör behandling av personuppgifter som utförs av statliga myndigheter som lyder under regeringen förhåller det sig annorlunda. Med undantag för de fall som avses i 2 kap. 6 § andra stycket RF kan sådana föreskrifter som direkt eller indirekt rör behandling av personuppgifter meddelas av regeringen med stöd av dess restkompetens enligt 8 kap. 7 § första stycket 2 RF. Vidare kan sektorsspecifika föreskrifter som reglerar kommunala myndigheters eller enskilda organs behandling av personuppgifter meddelas med stöd av bemyndiganden i annan lag än dataskyddslagen. Det kommer följaktligen även i fortsättningen att finnas både lagar och förordningar som innehåller bestämmelser som rör behandling av personuppgifter. Dessa bestämmelser kommer i första hand att komplettera dataskyddsförordningen, men kan i vissa fall avse frågor som också regleras i dataskyddslagen. Det kan vara bestämmelser som direkt rör behandling av personuppgifter, t.ex. om möjligheten att behandla känsliga personuppgifter i en viss verksamhet. Bestämmelserna kan också indirekt röra behandling av personuppgifter, t.ex. skyldigheter att lämna ut vissa uppgifter eller särskilda förfaranderegler. Sådana bestämmelser i såväl lagar som förordningar som avviker från dataskyddslagen bör, på motsvarande sätt som gällt i förhållande till personuppgiftslagen, ha företräde framför bestämmelserna i dataskyddslagen.

Bestämmelser som rör behandling av personuppgifter kan också förekomma i andra EU-förordningar än dataskyddsförordningen. I Sverige jämställs sådana förordningar med lag och kommer därmed, på samma sätt som lagar beslutade av riksdagen, att ha företräde framför dataskyddslagen. Det finns enligt regeringens mening inte skäl att, som *Kungliga tekniska högskolan* förordar, särskilt ange detta i lagtexten.

Regeringen anser att den bestämmelse som anger att dataskyddslagen är subsidiär till avvikande bestämmelser i annan författning bör utformas på samma sätt som 4 § i den nya förvaltningslagen (2017:900). Detta innebär ingen saklig skillnad jämfört med den formulering som används i personuppgiftslagen. Det bör dock betonas att den bestämmelse om

subsidiaritet som föreslås i dataskyddslagen kommer att få en betydligt mer begränsad betydelse än dess motsvarighet i 2 § PUL, även om dess innebörd är densamma. Detta beror på att dataskyddslagen, till skillnad från personuppgiftslagen, inte är heltäckande. Dataskyddslagen utgör endast ett komplement till dataskyddsförordningen och reglerar bara vissa frågor. Bestämmelsen om att annan lag eller förordning ska ha företräde framför dataskyddslagen utvidgar inte utrymmet för att göra nationella undantag från de direkt tillämpliga bestämmelserna i dataskyddsförordningen. Principen om unionsrättens företräde innebär att en bestämmelse i en sektorsspecifik författning får tillämpas endast om den är förenlig med dataskyddsförordningen och avser en fråga som enligt förordningen får särregleras eller specificeras genom nationell rätt. Det finns enligt regeringens mening inte skäl att, som *Sveriges advokatsamfund* förespråkar, ange detta särskilt i lagtexten.

6 Tillämpningsområdet

6.1 Behandling av personuppgifter utanför dataskyddsförordningens tillämpningsområde

6.1.1 Förordningens tillämpningsområde utsträcks

Regeringens förslag: EU:s dataskyddsförordning, i tillämpliga delar, och dataskyddslagen ska gälla även i verksamhet utanför unionsrättens tillämpningsområde och vid Sveriges deltagande i den gemensamma utrikes- och säkerhetspolitiken. Detta ska dock inte gälla i verksamhet som omfattas av lagen om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst, lagen om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet eller 6 kap. polisdatalagen.

Utredningens förslag överensstämmer delvis med regeringens. Utredningen föreslår inte något undantag. Vidare har utredningens förslag en annan språklig utformning.

Remissinstanserna: Det stora flertalet remissinstanser tillstyrker utredningens förslag eller har inga synpunkter på det. *Förvaltningsrätten i Stockholm* och *Centrala studiestödsnämnden* efterfrågar dock fördjupade överväganden i denna del. *Försvarsmakten* motsätter sig att förordningen ska vara tillämplig i verksamhet som omfattas av lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst. *Försvarets radioanstalt* anser att det bör framgå av lagen att dataskyddsförordningen inte gäller i verksamhet som omfattas av lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet. *Sveriges advokatsamfund* ifrågasätter utvidgningen i den del som avser den gemensamma utrikes- och säkerhetspolitiken och menar att regleringen kan komma i konflikt med

framtida bestämmelser inom det området som beslutas av rådet. *Lunds universitet* anser att det behövs en mer utförlig motivering till att förordningens tillämpningsområde utvidgas till att omfatta även den gemensamma utrikes- och säkerhetspolitiken. Försvarsmakten, Lunds universitet och Sveriges advokatsamfund anser att det av lagtexten ska framgå vilka delar av dataskyddsförordningen som ska gälla utanför dess tillämpningsområde. Ytterligare ett par remissinstanser, bl.a. Centrala studiestödsnämnden, påpekar att den föreslagna utformningen av bestämmelsen kan medföra tillämpningssvårigheter.

Skälen för regeringens förslag

Dataskyddsförordningens tillämpningsområde bör utsträckas…

Dataskyddsdirektivet gäller inte för sådan behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av gemenskapsrätten, exempelvis sådan verksamhet som avses i avdelningarna V och VI i fördraget om Europeiska unionen, och inte under några omständigheter behandlingar som rör allmän säkerhet, försvar, statens säkerhet (inbegripet statens ekonomiska välstånd när behandlingen har samband med frågor om statens säkerhet) och statens verksamhet på straffrättens område. Personuppgiftslagen är däremot generellt tillämplig, vilket innebär att den också gäller för sådan behandling som faller utanför det nuvarande dataskyddsdirektivets tillämpningsområde.

Dataskyddsförordningen har, i likhet med dataskyddsdirektivet, ett begränsat tillämpningsområde. Enligt artikel 2.2 a ska förordningen inte tillämpas på behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av unionsrätten. I skäl 16 till dataskyddsförordningen anges verksamhet rörande nationell säkerhet som ett exempel på en sådan verksamhet. Dataskyddsförordningen ska enligt artikel 2.2 b inte heller tillämpas på behandling av personuppgifter som medlemsstaterna utför när de bedriver verksamhet som omfattas av den gemensamma utrikes- och säkerhetspolitiken.

EU-domstolen har ansett att dataskyddsdirektivet ska ha ett brett tillämpningsområde, se dom Lindqvist, C-101/01, EU:C:2003:596, punkterna 34–35 och 44. Det finns ingenting i dataskyddsförordningen som antyder att unionslagstiftaren har avsett att inskränka det materiella tillämpningsområdet för dataskyddsförordningen jämfört med direktivet. Exakt vilka verksamheter som faller utanför unionsrättens tillämpningsområde och därmed inte omfattas av förordningens bestämmelser om behandling av personuppgifter är dock inte helt klart, förutom när det gäller verksamhet rörande nationell säkerhet som uttryckligen nämns i skälen. Även en restriktiv tolkning av undantaget från förordningens tillämpningsområde bör emellertid innebära att det inom den offentliga sektorn också finns annan verksamhet som faller utanför unionsrättens tillämpningsområde.

Anledningen till att personuppgiftslagen gjordes generellt tillämplig var bl.a. att det ansågs särskilt viktigt med ett starkt integritetsskydd för personuppgifter inom all offentlig verksamhet. Vidare ansågs den lösningen garantera att behovet av särregler i förhållande till personuppgiftslagen alltid övervägs noga i den ordning som krävs för författ-

ningsgivning (prop. 1997/98:44 s. 40–41). Dessa skäl är enligt regeringens bedömning alltjämt aktuella.

Sverige har vidare gjort vissa andra internationella åtaganden att skydda enskilda individers personliga integritet. Sverige har bl.a. tillträtt Europarådets dataskyddskonvention (CETS 108) som ställer krav på att konventionsstaterna har en generellt tillämplig reglering om dataskydd. När personuppgiftslagen upphävs måste det därför införas en reglering om dataskydd för det område som inte omfattas av det nya EU-regelverket. Utredningen föreslår att detta ska åstadkommas genom att dataskyddsförordningen görs tillämplig inom detta område.

Vissa remissinstanser, bl.a. *Centrala studiestödsnämnden* och *Förvaltningsrätten i Stockholm*, efterlyser en mer utförlig motivering till förslaget. Som konstateras ovan är det vanskligt att bedöma närmare var gränserna för unionsrättens tillämpningsområde går. Det är därför svårt att klart avgränsa vilka verksamheter som behöver en komplett nationell dataskyddsreglering. Dessa svårigheter kan undvikas med utredningens förslag. Att utsträcka förordningens tillämpningsområde har också den fördelen att en myndighet som ägnar sig både åt verksamhet som faller inom unionsrättens tillämpningsområde och verksamhet som skulle kunna anses falla utanför denna, inte behöver definiera denna gräns utan i stället kan tillämpa ett och samma regelverk.

Sveriges advokatsamfund anser att det är vanskligt att utvidga dataskyddsförordningens tillämpning till den gemensamma utrikes- och säkerhetspolitiken, eftersom rådet med stöd av artikel 39 i fördraget om Europeiska unionen har befogenhet att anta beslut om bestämmelser om behandling av personuppgifter i medlemsstaterna på detta område. Det kan dock konstateras att rådet ännu inte har antagit några sådana bestämmelser. För det fall att rådet skulle göra det kan detta hanteras genom att bestämmelser som avviker från dataskyddslagen tas in i en förordning beslutad av regeringen. Regeringen bedömer därför att de farhågor som Sveriges advokatsamfund hyser inte utgör skäl att frångå utredningens förslag.

Regeringen anser sammanfattningsvis, i likhet med utredningen, att förordningens bestämmelser om behandling av personuppgifter bör utsträckas till att gälla även vid sådan behandling av personuppgifter som enligt artikel 2.2 a och b inte omfattas av dataskyddsförordningens tillämpningsområde. Bestämmelserna i dataskyddslagen bör också gälla i dessa fall. Se dock nedan om avgränsning och undantag samt avsnitt 18 om ikraftträdande- och övergångsbestämmelser.

… i tillämpliga delar

Utredningen föreslår att dataskyddsförordningen ska gälla i tillämpliga delar inom det utsträckta tillämpningsområdet. Anledningen till detta är att det finns bestämmelser i förordningen som inte kan tillämpas utanför dess egentliga tillämpningsområde. Som utredningen påpekar är det inte möjligt att i nationell rätt ålägga tillsynsmyndigheter i andra länder att samarbeta med den svenska tillsynsmyndigheten. De bestämmelser som ålägger tillsynsmyndigheterna en skyldighet att samarbeta är således inte tillämpliga. Däremot finns det förstås ingenting som hindrar att den svenska tillsynsmyndigheten söker sådant samarbete, om det i det

enskilda fallet skulle vara värdefullt. Vidare är det inte möjligt att genom nationell rätt ge Europeiska dataskyddsstyrelsen behörighet att t.ex. utfärda riktlinjer och rekommendationer inom det område där EU inte har befogenheter i enlighet med fördragen. Det är inte heller möjligt att ge kommissionen rätt att anta delegerade akter eller att ålägga kommissionen andra uppgifter.

De bestämmelser i förordningen som avser andra medlemsstaters samarbetsskyldighet samt kommissionens och styrelsens uppgifter och befogenheter är således inte tillämpliga i detta avseende. Det rör sig framför allt om kapitel VII och kapitel X, men det finns även bestämmelser i andra delar av dataskyddsförordningen som på motsvarande sätt inte kan tillämpas i rent nationella sammanhang. Som exempel kan nämnas bestämmelserna som rör uppförandekoder och certifiering, till den del de avser kommissionens och styrelsens roll (t.ex. artiklarna 40.11 och 42.8). De bestämmelser som ger kommissionen befogenheter i fråga om överföring till tredjeland (artikel 45) är inte heller tillämpliga, liksom bestämmelserna som ålägger kommissionen skyldigheter i fråga om uppföljande åtgärder (artiklarna 97 och 98). Regeringen anser inte, till skillnad från *Försvarsmakten*, *Lunds universitet* och *Sveriges advokatsamfund*, att det är lämpligt att i detalj ange i lagtexten vilka bestämmelser i förordningen som är tillämpliga.

Enligt regeringens bedömning bör den föreslagna ordningen inte föranleda några tillämpningssvårigheter som *Centrala studiestödsnämnden* befarar, eftersom det inte råder något tvivel om att alla materiella bestämmelser som rör den registrerades rättigheter och den personuppgiftsansvariges skyldigheter och ansvar kan tillämpas.

Viss verksamhet bör undantas från det utsträckta tillämpningsområdet

I avsnitt 5.1.3 föreslår regeringen att dataskyddslagen ska vara subsidiär till avvikande bestämmelser i annan lag eller i förordning. Det är således möjligt att genom sektorsspecifik författning göra undantag från den föreslagna bestämmelsen om utsträckt tillämpning av dataskyddsförordningens bestämmelser, om det för en viss verksamhet anses vara mer lämpligt med en heltäckande nationell reglering. Det finns också möjlighet att i en sådan författning göra undantag endast från vissa bestämmelser i dataskyddsförordningen som inte bör gälla i den aktuella verksamheten. Detta motsvarar den ordning som gäller i dag, eftersom personuppgiftslagen är generellt tillämplig men subsidiär till avvikande bestämmelser i annan lag eller förordning.

Det finns inom det utsträckta tillämpningsområdet ett fåtal författningar som avser behandling av personuppgifter i verksamhet som rör nationell säkerhet. Dessa avser bl.a. behandling av personuppgifter hos Försvarsmakten (lagen om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst) och Försvarets radioanstalt (lagen om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet). Båda dessa författningar gäller i stället för personuppgiftslagen. Utanför lagarnas respektive tillämpningsområden tillämpas dock personuppgiftslagen hos Försvarsmakten och Försvarets radioanstalt. Lagarna

är för närvarande föremål för översyn, men detta arbete kommer inte att vara slutfört den 25 maj 2018.

Inom det utsträckta tillämpningsområdet för dataskyddsförordningen ligger också delar av Säkerhetspolisens verksamhet. Behandling av personuppgifter i denna verksamhet, som rör nationell säkerhet, regleras av 6 kap. polisdatalagen (2010:361). Utredningen om 2016 års dataskyddsdirektiv (Ju 2016:06) föreslår i sitt slutbetänkande, SOU 2017:74, att det ska införas en ny lag om Säkerhetspolisens behandling av personuppgifter och att 6 kap. polisdatalagen ska upphävas. Utredningen bedömer att Säkerhetspolisens verksamhet är av sådan karaktär att det med hänsyn både till effektivitets- och integritetsskäl krävs en reglering som avviker från dataskyddsförordningen. Utredningen föreslår därför att dataskyddslagen, och därmed den bestämmelse som utsträcker dataskyddsförordningens tillämpningsområde, inte ska gälla vid behandling som rör nationell säkerhet i Säkerhetspolisens brottsbekämpande och lagförande verksamhet. Förslaget är för närvarande föremål för beredning inom Regeringskansliet, men kommer inte att vara genomfört den 25 maj 2018.

Regeringen anser att det med hänsyn till rikets säkerhet inte är lämpligt att låta dataskyddsförordningen bli tillämplig även inom de mest känsliga verksamhetsområdena innan den pågående översynen av författningarna på försvarsområdet och beredningen av förslagen rörande Säkerhetspolisen har avslutats. Detta bör, som *Försvarsmakten* och *Försvarets radioanstalt* förordar, åstadkommas genom undantag från den bestämmelse som utsträcker dataskyddsförordningens tillämpningsområde. I verksamhet som omfattas av lagen om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst, lagen om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet samt 6 kap. polisdatalagen bör därför den bestämmelse som utsträcker dataskyddsförordningens tillämpningsområde inte gälla. Frågan har beretts med *Säkerhetspolisen*, *Datainspektionen*, *Säkerhets- och integritetsskyddsnämnden*, Försvarsmakten, Försvarets radioanstalt, *Totalförsvarets rekryteringsmyndighet* och *Myndigheten för samhällsskydd och beredskap*, som inte invänder mot förslaget.

Sammanfattande bedömning

Regeringen anser således i likhet med utredningen att bestämmelserna i dataskyddsförordningen, i tillämpliga delar, och i dataskyddslagen bör gälla även vid behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av unionsrätten och i verksamhet som omfattas av avdelning V kapitel 2 i fördraget om Europeiska unionen. Dataskyddsförordningen och dataskyddslagen bör dock inte gälla i verksamhet som omfattas av lagen om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst, lagen om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet samt 6 kap. polisdatalagen.

Sverige har inte överlåtit beslutskompetens till EU inom de områden där dataskyddsförordningens bestämmelser ska gälla enligt förslaget i

denna del. Om förordningen ändras bör därför den svenska lagstiftaren ta ställning till om dessa ändringar ska få genomslag även på de områden som är undantagna från förordningens tillämpningsområde. Hänvisningen till förordningen i den nu aktuella bestämmelsen i dataskyddslagen bör därför vara statisk, dvs. avse den ursprungliga lydelsen av förordningen.

6.1.2 Bestämmelserna om personuppgiftsincidenter ska inte gälla om incidenten rör rikets säkerhet

Regeringens förslag: Bestämmelserna i EU:s dataskyddsförordning om anmälan till tillsynsmyndigheten av en personuppgiftsincident samt information till den registrerade om en sådan incident ska inte tillämpas i fråga om incidenter som ska rapporteras enligt säkerhetsskyddslagen eller föreskrifter som har meddelats i anslutning till den lagen.

Utredningen föreslår inte något sådant undantag.

Remissinstanserna: *Säkerhetspolisen*, *Försvarsmakten* och *Försvarets radioanstalt* invänder mot utredningens förslag i den del detta innebär att dataskyddsförordningens bestämmelser om personuppgiftsincidenter ska tillämpas utanför förordningens egentliga tillämpningsområde.

Skälen för regeringens förslag

Förordningens reglering rörande personuppgiftsincidenter

En personuppgiftsincident är enligt definitionen i artikel 4.12 i dataskyddsförordningen en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats. Om en sådan incident inträffar ska den personuppgiftsansvarige utan onödigt dröjsmål och, om så är möjligt, inte senare än 72 timmar efter att ha fått vetskap om den, anmäla incidenten till tillsynsmyndigheten (artikel 33). Undantag från denna anmälningsskyldighet gäller endast om det är osannolikt att incidenten medför en risk för fysiska personers rättigheter och friheter. Anmälan ska åtminstone a) beskriva personuppgiftsincidentens art, inbegripet, om så är möjligt, de kategorier av och det ungefärliga antalet registrerade som berörs samt de kategorier av och det ungefärliga antalet personuppgiftsposter som berörs, b) förmedla namnet på och kontaktuppgifterna för dataskyddsombudet eller andra kontaktpunkter där mer information kan erhållas, c) beskriva de sannolika konsekvenserna av personuppgiftsincidenten, och d) beskriva de åtgärder som den personuppgiftsansvarige har vidtagit eller föreslagit för att åtgärda personuppgiftsincidenten, inbegripet, när så är lämpligt, åtgärder för att mildra dess potentiella negativa effekter.

Om personuppgiftsincidenten sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige utan onödigt dröjsmål informera den registrerade om personuppgifts-

incidenten (artikel 34). Informationen ska innehålla en tydlig och klar beskrivning av personuppgiftsincidentens art och åtminstone de upplysningar och åtgärder som avses i artikel 33.3 b, c och d. Information till den registrerade krävs dock inte om vissa särskilt angivna villkor är uppfyllda, t.ex. om den personuppgiftsansvarige har genomfört lämpliga tekniska och organisatoriska skyddsåtgärder och dessa åtgärder tillämpats på de personuppgifter som påverkades av personuppgiftsincidenten, i synnerhet sådana som ska göra uppgifterna oläsbara för alla personer som inte är behöriga att få tillgång till personuppgifterna, såsom kryptering.

Enligt artikel 23 får det i unionsrätten eller nationell rätt föreskrivas ytterligare undantag från skyldigheten att informera de registrerade om en personuppgiftsincident, förutsatt att en sådan begränsning sker med respekt för andemeningen i de grundläggande rättigheterna och friheterna och utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle i syfte att säkerställa vissa särskilt angivna intressen, t.ex. den nationella säkerheten eller försvaret.

Andra skyldigheter att anmäla incidenter

Skyldigheten att anmäla incidenter till tillsynsmyndigheten är en av nyheterna i dataskyddsförordningen. Någon motsvarighet finns således inte enligt personuppgiftslagen. Liknande rapporteringsskyldigheter finns däremot på andra områden i svensk rätt, bl.a. till skydd för rikets säkerhet.

Enligt 10 a § första stycket säkerhetsskyddsförordningen (1996:633) ska en myndighet skyndsamt anmäla vissa it-incidenter till den myndighet som enligt 39 § utövar tillsyn över säkerhetsskyddet, dvs. till Försvarsmakten eller Säkerhetspolisen. Rapporteringsskyldigheten gäller bl.a. om incidenten allvarligt kan påverka säkerheten i ett informationssystem där hemliga uppgifter behandlas i en omfattning som inte är ringa eller om incidenten allvarligt kan påverka säkerheten i ett informationssystem som särskilt behöver skyddas mot terrorism. Med uttrycket hemliga uppgifter avses i säkerhetsskyddsförordningen uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen och som rör rikets säkerhet.

Enligt 20 § förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap (krisberedskapsförordningen) ska en myndighet till Myndigheten för samhällsskydd och beredskap skyndsamt rapportera it-incidenter som inträffat i myndighetens informationssystem och som allvarligt kan påverka säkerheten i den informationshantering som myndigheten ansvarar för eller i tjänster som myndigheten tillhandahåller åt en annan organisation. Denna rapporteringsskyldighet omfattar dock inte sådana incidenter som ska rapporteras enligt 10 a § säkerhetsskyddsförordningen.

Utredningen om genomförande av NIS-direktivet (Ju 2016:11) föreslår i sitt betänkande (SOU 2017:36) en ny lag om informationssäkerhet för vissa tillhandahållare av samhällsviktiga tjänster och digitala tjänster. Förslaget innebär bl.a. att leverantörer av samhällsnyttiga tjänster utan onödigt dröjsmål ska rapportera incidenter som har en betydande inverkan på kontinuiteten i den samhällsviktiga tjänst som de tillhanda-

håller. Rapporteringen ska göras till Myndigheten för samhällsskydd och beredskap. Bestämmelserna i den föreslagna lagen ska emellertid inte tillämpas på verksamhet som är av betydelse för Sveriges säkerhet. Detta innebär att den rapportering av it-incidenter som myndigheter är skyldiga att göra enligt 10 a § säkerhetsskyddsförordningen även fortsättningsvis ska rapporteras enligt säkerhetsskyddsförordningen och inte enligt den nya lagen (SOU 2017:36 s. 95).

Utredningen om 2016 års dataskyddsdirektiv lämnar i sitt delbetänkande (SOU 2017:29) förslag till en ny brottsdatalag. Förslaget innebär bl.a. att en personuppgiftsincident ska anmälas till tillsynsmyndigheten, utom i de fall där incidenten rör nationell säkerhet. Om incidenten rör nationell säkerhet ska den personuppgiftsansvarige inte heller vara skyldig att underrätta den registrerade om incidenten. Utredningen om 2016 års dataskyddsdirektiv anför att behovet av att skydda hemliga uppgifter som rör Sveriges säkerhet är så viktigt att endast den myndighet som utövar tillsyn över säkerhetsskyddet ska få ta del av den. Även om den rapporteringen har ett annat syfte än rapporteringen av personuppgiftsincidenter, anser utredningen att behovet av skydd för uppgifter som rör Sveriges säkerhet väger tyngre än behovet av att skydda enskilda från eventuella intrång i den personliga integriteten. Eftersom nationell säkerhet ligger utanför direktivets tillämpningsområde anser utredningen att sådana personuppgiftsincidenter som ska anmälas enligt 10 a § säkerhetsskyddsförordningen inte bör anmälas till tillsynsmyndigheten (SOU 2017:29 s. 337).

Bör förordningens bestämmelser om personuppgiftsincidenter gälla i all verksamhet som inte omfattas av unionsrätten?

Av säkerhetsskyddsskäl måste det, vilket *Säkerhetspolisen* framhåller, ställas höga krav på informationssäkerheten för uppgifter som kan avslöja svagheter i skyddet av uppgifter som rör rikets säkerhet eller mot terrorism, i synnerhet när uppgifterna kan ge en samlad bild av sådana svagheter. Som *Försvarsmakten* påpekar kommer dokumentation kring incidenter att visa på sårbarheter i berörda system och kan t.ex. visa på hur man kan kringgå skyddsåtgärder för att få obehörig tillgång till systemen. Kunskap om en personuppgiftsincident kan på så vis ge en motståndare uppgifter som underlättar vidare angrepp och inhämtning. Sådana uppgifter bör därför inte spridas till fler myndigheter än vad som är nödvändigt.

Incidentrapporteringen enligt säkerhetsskyddsförordningen eller krisberedskapsförordningen tar visserligen inte främst sikte på säkerhetsincidenter där personuppgifter på olika sätt röjts. Oavsett anledningen till att en it-incident rapporteras syftar en sådan rapportering till att uppmärksamma brister i skyddet av information för att därefter vidta åtgärder för att säkerställa detta. Om en it-incident inträffar i ett system med personuppgifter kommer alltså de skyddsåtgärder och säkerhetshöjande åtgärder som vidtas med anledning av incidenten att stärka skyddet även för personuppgifterna och därmed för den personliga integriteten.

Mot bakgrund av behovet av skydd för rikets säkerhet anser regeringen att det bör införas en begränsning i fråga om tillämpningen av data-

skyddsförordningen utanför dess egentliga tillämpningsområde, när det gäller bestämmelserna om personuppgiftsincidenter. Eftersom dataskyddsförordningen egentligen inte gäller i verksamhet som rör nationell säkerhet, finns det heller inga unionsrättsliga hinder mot en sådan begränsning.

Frågan har beretts med Säkerhetspolisen, *Datainspektionen*, *Säkerhets- och integritetsskyddsnämnden*, Försvarsmakten, *Försvarets radioanstalt*, *Totalförsvarets rekryteringsmyndighet* och *Myndigheten för samhällsskydd och beredskap*, som i sak delar bedömningen att dataskyddsförordningens bestämmelser om anmälan och information om personuppgiftsincidenter inte bör gälla för incidenter som rör nationell säkerhet. Datainspektionen anser emellertid att bestämmelsen i artikel 33.5 om skyldighet att dokumentera incidenter ska gälla även i dessa fall. Regeringen, som i och för sig instämmer i att även incidenter som rör nationell säkerhet bör dokumenteras, anser dock att dataskyddsförordningens dokumentationsskyldighet inte bör gälla i fråga om incidenter som inte ska rapporteras enligt det regelverket.

När det gäller frågan om hur ett undantag från rapporteringsskyldigheten bör utformas har regeringen övervägt flera alternativ. I förslaget till brottsdatalag anges att anmälningsskyldighet inte gäller incidenter som rör nationell säkerhet. En liknande formulering återfinns även i skäl 16 till dataskyddsförordningen, som ett exempel på verksamhet som inte omfattas av unionsrätten. Det skulle mot den bakgrunden kunna anges i dataskyddslagen att artiklarna 33 och 34 i dataskyddsförordningen inte ska gälla personuppgiftsincidenter som rör nationell säkerhet. Det finns dock, som Säkerhetspolisen anför, en risk för att det skulle innebära tillämpningssvårigheter, eftersom andra begrepp används i svensk rätt rörande samma sak. Som exempel kan nämnas att begreppet rikets säkerhet används i säkerhetsskyddslagen (1996:627). Det begreppet har dock i svensk rätt successivt ersatts av uttrycket Sveriges säkerhet, bl.a. i 19 kap. brottsbalken. I regeringens lagrådsremiss, Ett modernt och stärkt skydd för Sveriges säkerhet – ny säkerhetsskyddslag, föreslås att uttrycket Sveriges säkerhet ska ersätta rikets säkerhet även i säkerhetsskyddslagen.

Säkerhetspolisen och Försvarets radioanstalt föreslår i sina remissvar över betänkandet att det av dataskyddslagen bör framgå att artiklarna 33 och 34 i dataskyddsförordningen inte ska gälla personuppgiftsincidenter som ska rapporteras enligt 10 a § säkerhetsskyddsförordningen. Regeringen anser dock inte att det är lämpligt att i lag hänvisa till en förordning. Undantaget bör i stället ange att artiklarna 33 och 34 inte ska tillämpas i fråga om incidenter som ska rapporteras enligt säkerhetsskyddslagen eller föreskrifter som har meddelats i anslutning till den lagen.

6.2 Dataskyddslagens tillämpning vid gränsöverskridande behandling

Regeringens förslag: Dataskyddslagen ska gälla för personuppgiftsansvariga och personuppgiftsbiträden som är etablerade i Sverige, i fråga om behandling av personuppgifter som utförs inom ramen för verksamhet som bedrivs vid verksamhetsställen här i landet. Lagen ska även gälla för personuppgiftsansvariga som är etablerade på en annan plats där svensk rätt gäller enligt folkrätten. Lagen ska också gälla för personuppgiftsansvariga och personuppgiftsbiträden som endast är etablerade i tredje land, om behandlingen har anknytning till utbjudande av varor eller tjänster till registrerade i Sverige eller övervakning av registrerades beteende i Sverige.

Dataskyddslagens reglering om barns samtycke till behandling av personuppgifter vid erbjudande av informationssamhällets tjänster ska gälla alla barn som bor i Sverige, oavsett var de personuppgiftsansvariga eller personuppgiftsbiträdena är etablerade.

Utredningen föreslår inte någon sådan bestämmelse.

Promemorians förslag överensstämmer i sak med regeringens.

Remissinstanserna: Det stora flertalet remissinstanser tillstyrker förslaget i promemorian eller har inga synpunkter på det. *Umeå universitet* är inte övertygat om att etableringslandsprincipen leder till färre problem och anser att frågan bör utredas grundligt. *Sveriges advokatsamfund* avstyrker förslaget i den del som innebär att effektlandsprincipen ska gälla som utgångspunkt för dataskyddslagens territoriella tillämpningsområde. *Förvaltningsrätten i Stockholm* uppfattar förslaget som att vissa situationer hamnar utanför tillämpningsområdet och efterlyser mer problematiserande överväganden kring det. *Lunds universitet* invänder mot uttrycket barn som bor i Sverige och förordar i stället uttrycket varaktigt vistas. Även *Uppsala universitet* invänder mot uttrycket barn som bor i Sverige. Universitet har också synpunkter på formuleringen på en plats där svensk rätt gäller enligt folkrätten och förordar som enligt folkrätten lyder under svensk rätt eller som enligt folkrätten ska följa svensk rätt.

Skälen för regeringens förslag

Dataskyddslagens territoriella tillämpningsområde bör regleras

Behandling av personuppgifter är i många fall en gränsöverskridande aktivitet. Det är t.ex. inte ovanligt att den som behandlar personuppgifter om personer i Sverige inte själv är etablerad genom ett verksamhetsställe i landet. På motsvarande sätt kan svenska företag och organisationer behandla personuppgifter om individer i andra länder utan att ha något verksamhetsställe där. I dessa situationer uppkommer fråga om vilket lands lag som ska tillämpas – den lag som gäller i den registrerades land (effektlandsprincipen) eller den lag som gäller i det land där den personuppgiftsansvarige är etablerad (etableringslandsprincipen). Dataskyddsförordningen innehåller inte några regler om vilken nationell rätt som ska gälla vid gränsöverskridande personuppgiftsbehandling.

Det är ur ett tillämpningsperspektiv viktigt att det står klart i vilka fall dataskyddslagen gäller vid gränsöverskridande behandling av personuppgifter. Utan reglering av det territoriella tillämpningsområdet kommer det att råda osäkerhet i denna fråga. Av rättssäkerhetsskäl bör det därför införas en uttrycklig bestämmelse om det territoriella tillämpningsområdet i dataskyddslagen.

En reglering som följer förordningens principer

Etableringslandsprincipen kan sägas vara utgångspunkten i dataskyddsförordningens reglering om det territoriella tillämpningsområdet (artikel 3.1 och 3.3). Ett val av etableringslandsprincipen som huvudregel för dataskyddslagens tillämpningsområde skulle således harmoniera väl med regleringen i förordningen. Till skillnad från *Umeå universitet* bedömer regeringen inte att en sådan ordning skulle riskera att leda till otillbörlig konkurrenspåverkan. Det kan också konstateras att personuppgiftslagens reglering om tillämpningsområdet utgår från etableringslandsprincipen (4 § PUL). Ett val av denna princip skulle således även innebära en kontinuitet i förhållande till den nuvarande regleringen.

Mot denna bakgrund bör etableringslandsprincipen gälla som utgångspunkt för dataskyddslagens territoriella tillämpningsområde. Det saknar därmed betydelse var behandlingen faktiskt utförs och var den registrerade befinner sig. Omvänt bör lagen, enligt huvudregeln, inte gälla för personuppgiftsansvariga som saknar verksamhetsställe i Sverige, även om de behandlar uppgifter om personer i Sverige.

I den svenska språkversionen av dataskyddsförordningen anges i artikel 3.1 att förordningen ska tillämpas på behandling av personuppgifter inom ramen för verksamhet som bedrivs av personuppgiftsansvariga och personuppgiftsbiträden som är etablerade i unionen eller på en plats där en medlemsstats nationella rätt gäller enligt folkrätten, oavsett om behandlingen utförs i unionen eller inte. Vid en jämförelse med andra språkversioner framgår dock att avsikten är att förordningen endast ska tillämpas vid behandling som sker inom ramen för den verksamhet som bedrivs på verksamhetsställen i unionen. Om en personuppgiftsansvarig är etablerad såväl inom som utanför unionen, ska förordningen således inte tillämpas på den behandling som sker endast inom ramen för den verksamhet som bedrivs vid verksamhetsstället i tredjeland. Justitiedepartementet har mot denna bakgrund gett in en begäran om korrigering av den svenska lydelsen av artikel 3.1 (Ju2016/00482/L6).

På motsvarande sätt bör lagen vara tillämplig endast i fråga om behandling som utförs inom ramen för den verksamhet som bedrivs vid ett verksamhetsställe i Sverige. Den bör således inte gälla för behandling som utförs endast inom ramen för verksamhet som den personuppgiftsansvarige bedriver vid ett verksamhetsställe i ett annat EU-land, även om den personuppgiftsansvarige också har ett verksamhetsställe i Sverige.

Förvaltningsrätten i Stockholm förstår förslaget på så sätt att både den behandling av personuppgifter som utförs av personuppgiftsansvariga med etablering i Sverige och verksamhetsställe i en annan medlemsstat och den behandling som utförs av de som har etablering i en annan medlemsstat och verksamhetsställe i Sverige faller utanför lagens

tillämpningsområde. Förvaltningsrättens synpunkter tycks bygga på uppfattningen att en personuppgiftsansvarig endast kan vara etablerad i ett land samt att en personuppgiftsansvarig kan ha ett verksamhetsställe i ett land utan att vara etablerad där. Regeringen finner mot den bakgrunden anledning att understryka att en personuppgiftsansvarig kan ha verksamhetsställen, och därmed vara etablerad, i flera stater. En personuppgiftsansvarig som har ett verksamhetsställe i Sverige anses således etablerad här. På motsvarande sätt kan en personuppgiftsansvarig inte anses etablerad i Sverige utan att ha ett verksamhetsställe här. Förslagets innebörd är att etablering i Sverige inte är en tillräcklig förutsättning för att lagen ska gälla. Lagen är nämligen tillämplig bara i fråga om behandling som utförs inom ramen för den verksamhet som bedrivs vid verksamhetsstället i Sverige.

Dataskyddsförordningen är enligt artikel 3.3 tillämplig på behandling av personuppgifter som utförs av en personuppgiftsansvarig som inte är etablerad i unionen, men på en plats där en medlemsstats nationella rätt gäller enligt folkrätten. Som exempel nämns i skäl 25 en medlemsstats diplomatiska beskickning eller konsulat. På motsvarande sätt bör dataskyddslagen vara tillämplig vid behandling av personuppgifter som utförs av personuppgiftsansvariga som inte är etablerade i Sverige, men som är etablerade på en plats där svensk rätt gäller enligt folkrätten, t.ex. vid svenska utlandsmyndigheter. *Uppsala universitet* invänder mot den föreslagna formuleringen och anser att ordet plats är alltför likt ordet ort, som avser en geografisk plats. Regeringen anser dock att den ordalydelse som används i förordningen också bör användas i lagen, för att det ska vara tydligt att innebörden är densamma.

Dataskyddsförordningen är i vissa fall tillämplig även för personuppgiftsansvariga och personuppgiftsbiträden som inte alls är etablerade inom EU. Enligt artikel 3.2 är förordningen tillämplig, trots att etablering inom unionen saknas, om behandlingen avser registrerade i unionen och har anknytning till antingen utbjudande av varor eller tjänster till registrerade i unionen eller övervakning av registrerades beteende i unionen. Enligt dataskyddsförordningen gäller således i dessa fall effektlandsprincipen. Eftersom dataskyddsförordningen måste kompletteras av nationell rätt, t.ex. i fråga om rättsmedel, kommer frågan att uppstå om vilken nationell lag som ska gälla. Det framstår i en sådan situation som lämpligast att den nationella regleringen utgår från samma princip som förordningen när det gäller personuppgiftsansvariga och personuppgiftsbiträden som inte är etablerade inom EU. Detta innebär att dataskyddslagen i sådana fall bör gälla vid behandling av personuppgifter som avser registrerade som befinner sig i Sverige, om behandlingen har anknytning till antingen utbjudande av varor eller tjänster till registrerade i Sverige eller övervakning av registrerades beteende i Sverige. Detta innebär i praktiken att dataskyddslagen kommer att gälla i de situationer då dataskyddsförordningen är tillämplig i fråga om behandling som avser registrerade i Sverige och som utförs av personuppgiftsansvariga som endast är etablerade i tredjeland.

Sveriges advokatsamfund förordar att etableringsprincipen ska gälla även i fråga om behandling som utförs av en personuppgiftsansvarig som inte är etablerad i unionen och som omfattas av dataskyddsförordningen enligt artikel 3.2. Advokatsamfundet påpekar att frågan om den territo-

riella räckvidden hos dataskyddsdirektivet inom den närmaste tiden kommer att prövas av EU-domstolen och att prövningen kan resultera i att EU-domstolen konstaterar att en utsträckning av tillämpningsområdet utanför unionen kommer i konflikt med folkrätten (mål nr C-136/17). Regeringen kan i det sammanhanget konstatera att dataskyddslagen kompletterar dataskyddsförordningen och kan alltså inte tillämpas självständigt. Om dataskyddsförordningen inte skulle vara tillämplig i de situationer som avses i artikel 3.2 kommer inte heller en tillämpning av dataskyddslagen att kunna aktualiseras.

Samma åldersgräns för samtycke bör gälla för alla barn som bor i Sverige

Regeringen föreslår i avsnitt 9 att barn som har fyllt 13 år själva ska kunna lämna samtycke till behandling av personuppgifter vid erbjudande av informationssamhällets tjänster. Bestämmelsen utgör ett undantag från den 16-årsgräns som regleras i artikel 8 i dataskyddsförordningen. Denna bestämmelses tillämpningsområde bör inte följa etableringslandsprincipen, eftersom det skulle kunna leda till olika åldersgränser för barn i Sverige beroende på vilken åldersgräns som valts i tjänsteleverantörens etableringsland. Det skulle också kunna leda till otillbörliga lättnader för företag och organisationer som är etablerade i Sverige och som riktar sig till barn i andra länder. Dessutom vore det olämpligt av Sverige att införa en sänkt åldersgräns som skulle kunna åberopas vid personuppgiftsbehandling avseende barn i andra medlemsstater, där lagstiftaren gjort en annan bedömning av vilken åldersgräns som bör gälla.

Mot denna bakgrund bör bestämmelsen om barns samtycke gälla vid behandling av personuppgifter som avser barn som bor i Sverige, oavsett var de personuppgiftsansvariga eller deras biträden är etablerade. Detta hindrar inte det fria flödet av personuppgifter, eftersom den sänkta åldersgränsen utgör en lättnad för de personuppgiftsansvariga i förhållande till deras skyldigheter enligt förordningen.

Lunds universitet och *Uppsala universitet* anser att uttrycket bor i Sverige är alltför vagt. Regeringen anser dock att det i detta sammanhang är angeläget att använda ett uttryck som var och en förstår innebörden av, inte minst de barn som berörs av bestämmelsen. Begreppet bor är av det skälet att föredra framför varaktigt vistas eller hemvist. Som framgår av promemorian ska ett barn inte anses bo i Sverige om det endast är på genomresa eller besök i landet. Detta torde också överensstämma med hur begreppet bor används i vanligt språkbruk. Det ska däremot inte krävas att barnet är folkbokfört i landet, att det redan har vistats i Sverige under en viss tidsperiod eller att det har beviljats uppehållstillstånd här. Även asylsökande barn i Sverige omfattas således av bestämmelsen.

7 Förhållandet till yttrande- och informationsfriheten

7.1 Förhållandet till tryckfrihetsförordningen och yttrandefrihetsgrundlagen förtydligas

Regeringens förslag: EU:s dataskyddsförordning och dataskyddslagen ska inte tillämpas i den utsträckning det skulle strida mot tryckfrihetsförordningen eller yttrandefrihetsgrundlagen.

Utredningens förslag överensstämmer i huvudsak med regeringens. Utredningen föreslår att dataskyddsförordningen och dataskyddslagen inte ska tillämpas i den utsträckning det skulle strida mot bestämmelserna om tryck- och yttrandefrihet i tryckfrihetsförordningen eller yttrandefrihetsgrundlagen.

Remissinstanserna: Det stora flertalet remissinstanser tillstyrker förslaget eller har inga synpunkter på det. Flera remissinstanser, bl.a. *Vetenskapsrådet*, *Landsorganisationen i Sverige*, *Sveriges akademikers centralorganisation*, *Sveriges Ingenjörer*, *Myndigheten för press, radio och TV*, *Tidningsutgivarna* och *Stiftelsen Svenska Filminstitutet*, lyfter särskilt fram vikten av en tydlig reglering om undantag för grundlagsskyddad verksamhet. *Mörbylånga kommun* påpekar att frågor om förhållandet mellan personuppgiftslagen och offentlighetsprincipen fortfarande dyker upp i verksamheten. *Forskningsrådet för hälsa, arbetsliv och välfärd* framhåller att det är ytterst angeläget att den svenska offentlighetsprincipen inte förändras av dataskyddslagen. *Datainspektionen* ifrågasätter förslagets förenlighet med EU-rätten och föreslår att bestämmelsen ska utgå. Enligt Datainspektionen ger dataskyddsförordningen inte utrymme för ett sådant generellt undantag i nationell rätt som föreslås. Datainspektionen framhåller vidare att myndigheten tidigare påpekat de risker som grundlagsskyddet medför för integritetsskyddet, särskilt avseende personuppgiftsbehandling på internet som omfattas av utgivningsbevis för databaser. *Kommerskollegium*, som delar utredningens bedömning om att undantag från vissa av dataskyddsförordningens bestämmelser får göras, ifrågasätter upplysningsbestämmelsens breda formulering och menar att den kan strida mot principen om EU-rättens företräde. *Södertörns tingsrätt* anser att ökad digitalisering och utveckling av vissa typer av databaser ger anledning till inskränkningar på det grundlagsskyddade området och hänvisar bl.a. till de förslag som lämnas i betänkandet Ändrade mediegrundlagar (SOU 2016:58). *Stiftelsen för internetinfrastruktur* anser att utredningens förslag inte löser problemet med att aktörer ansöker om utgivningsbevis för webbplatser för att undkomma personuppgiftslagens bestämmelser, t.ex. för behandling av personuppgifter som rör lagöverträdelser.

Skälen för regeringens förslag: Enligt artikel 9 i dataskyddsdirektivet ska medlemsstaterna, med avseende på behandling av personuppgifter som sker uteslutande för journalistiska ändamål eller konstnärligt eller litterärt skapande, besluta om undantag och avvikelser från delar av direktivet endast om de är nödvändiga för att förena rätten till privatlivet

med reglerna om yttrandefriheten. Vid genomförandet av dataskyddsdirektivet gjorde regeringen bedömningen att tryckfrihetsförordningen och yttrandefrihetsgrundlagen inte behövde ändras (prop. 1997/98:44 s. 50). I 7 § första stycket PUL infördes en upplysningsbestämmelse som anger att bestämmelserna i lagen inte ska tillämpas i den utsträckning det skulle strida mot bestämmelserna om tryck- och yttrandefrihet i tryckfrihetsförordningen och yttrandefrihetsgrundlagen. Det innebär bl.a. att de grundlagsskyddade rättigheterna att framställa och sprida yttranden samt meddelar- och anskaffarfriheten undantas från personuppgiftslagens tillämpningsområde.

I dataskyddsförordningen regleras förhållandet till yttrande- och informationsfriheten i artikel 85.1. Där anges att medlemsstaterna i sin nationella lagstiftning ska förena rätten till integritet i enlighet med förordningen med rätten till yttrande- och informationsfrihet, inbegripet personuppgiftsbehandling för journalistiska ändamål samt för akademiskt, konstnärligt eller litterärt skapande. Vid behandling för sådana ändamål ska medlemsstaterna enligt artikel 85.2 föreskriva om undantag eller avvikelser från i artikeln angivna delar av förordningens bestämmelser, om det är nödvändigt för att förena rätten till integritet med yttrande- och informationsfriheten.

Enligt regeringens bedömning ger regleringen i artikel 85 i dataskyddsförordningen ett något större utrymme för undantag än direktivet, bl.a. genom att det inte längre krävs att behandling ska ske uteslutande för journalistiska ändamål för att undantag ska kunna göras. Därutöver anger skäl 153 att begreppet yttrandefrihet måste ges en bred tolkning för att beakta vikten av rätten till yttrandefrihet i varje demokratiskt samhälle. Regeringen bedömer mot denna bakgrund, till skillnad från *Datainspektionen* och *Kommerskollegium*, att den unionsrättsliga dataskyddsregleringen även fortsättningsvis ger utrymme för bestämmelserna om tryck- och yttrandefrihet i tryckfrihetsförordningen och yttrandefrihetsgrundlagen. Med anledning av *Södertörns tingsrätts* och Datainspektionens synpunkter kan framhållas att regeringen i propositionen Ändrade mediegrundlagar (prop. 2017/18:49) gör bedömningen att det med hänsyn till skyddet för den personliga integriteten finns skäl att begränsa grundlagsskyddet för vissa söktjänster som innehåller personuppgifter av särskilt integritetskänslig karaktär. I propositionen föreslår regeringen därför att det införs bestämmelser i tryckfrihetsförordningen och yttrandefrihetsgrundlagen som ger utrymme att under vissa förutsättningar i lag föreskriva om förbud mot offentliggörande av sådana personuppgifter, om de är tillgängliga på ett sätt som innebär särskilda risker för intrång i enskildas personliga integritet.

Frågan är då om det finns behov av en bestämmelse i dataskyddslagen som tydliggör förhållandet mellan dataskyddsförordningen och bestämmelserna om tryck- och yttrandefrihet i tryckfrihetsförordningen och yttrandefrihetsgrundlagen. Som utredningen och flera remissinstanser konstaterar är det angeläget att dataskyddsförordningens och dataskyddslagens bestämmelser inte ger upphov till osäkerhet kring möjligheterna till personuppgiftsbehandling på det grundlagsskyddade området. En sådan osäkerhet skulle kunna påverka vitala delar av opinionsskapande verksamhet som är av grundläggande betydelse för demokratin. Som utredningen konstaterar innebär det förhållandet att den unionsrättsliga

dataskyddsregleringen är en direkt tillämplig förordning, som dessutom kan leda till kännbara sanktionsavgifter, ett än större behov av ett förtydligande av förhållandet till tryck- och yttrandefrihetsregleringen. Regeringen instämmer därför i utredningens bedömning att det bör införas en bestämmelse som tydliggör att dataskyddsförordningen och dataskyddslagen inte ska tillämpas i den utsträckning det skulle strida mot grundlagsregleringen om tryck- och yttrandefrihet.

Utredningen föreslår inte att det ska införas någon bestämmelse om dataskyddsregelverkets förhållande till handlingsoffentligheten. Som bl.a. *Mörbylånga kommun* ger uttryck för är det emellertid angeläget att även förhållandet mellan dataskyddsregelverket och offentlighetsprincipen är tydligt. Förhållandet till offentlighetsprincipen regleras i dag i skäl 72 i dataskyddsdirektivet, där det anges att det är möjligt att vid genomförandet av direktivet ta hänsyn till principen om allmänhetens tillgång till allmänna handlingar. Som framgår ovan gjorde regeringen vid genomförandet av dataskyddsdirektivet bedömningen att tryckfrihetsförordningen inte behövde ändras. I 8 § PUL infördes en bestämmelse som förtydligade förhållandet till offentlighetsprincipen. Av bestämmelsen framgår att lagens bestämmelser inte ska tillämpas i den utsträckning det skulle inskränka en myndighets skyldighet att enligt 2 kap. TF lämna ut personuppgifter.

I dataskyddsförordningen regleras förhållandet till offentlighetsprincipen i artikel 86. Där anges att personuppgifter i allmänna handlingar som förvaras av en myndighet, ett offentligt organ eller ett privat organ för utförande av en uppgift av allmänt intresse får lämnas ut av myndigheten eller organet i enlighet med medlemsstatens nationella lagstiftning för att jämka samman allmänhetens rätt att få tillgång till allmänna handlingar med rätten till skydd för personuppgifter i enlighet med förordningen. Förordningens artikel 86 innebär till sin ordalydelse en något mer omfattande reglering än motsvarande bestämmelse i personuppgiftslagen, eftersom även offentliga organ och privata organ som förvarar allmänna handlingar för utförande av en uppgift av allmänt intresse omfattas. Av skäl 154 i förordningen framgår att allmänhetens rätt att få tillgång till handlingar kan betraktas som ett allmänt intresse och att handlingarna bör kunna lämnas ut offentligt om utlämning stadgas i den nationella lagstiftningen. Vidare anges att den nationella rätten bör sammanjämka allmänhetens rätt att få tillgång till allmänna handlingar och vidareutnyttjande av information från den offentliga sektorn med rätten till skydd för personuppgifter samt att nationell lagstiftning därför får innehålla föreskrifter om den nödvändiga sammanjämkningen med rätten till skydd för personuppgifter enligt förordningen.

Enligt regeringens bedömning ger regleringen i förordningen ett ännu tydligare stöd än dataskyddsdirektivet för att den EU-rättsliga dataskyddsregleringen inte inkräktar på den grundlagsreglerade offentlighetsprincipen. Den nödvändiga sammanjämkning som avses i dataskyddsförordningen kommer i svensk rätt till uttryck bl.a. genom bestämmelserna i offentlighets- och sekretesslagen, som är resultatet av noggranna avvägningar mellan allmänhetens intresse av insyn i det allmännas verksamhet och den enskildes behov av skydd för sin personliga integritet. Det tydliga stöd som dataskyddsförordningen ger skulle kunna tala för att något ytterligare förtydligande i nationell rätt

inte behövs. Som konstateras ovan innebär dock det förhållandet att den unionsrättsliga dataskyddsregleringen är en direkt tillämplig förordning, som dessutom kan leda till kännbara sanktionsavgifter, att behovet av att klargöra förhållandet till grundlagarna blir ännu tydligare än i dag. Regeringen anser mot denna bakgrund att det i dataskyddslagen bör tydliggöras att dataskyddsförordningen och dataskyddslagen inte ska tillämpas i den utsträckning det skulle strida mot bestämmelserna om offentlighetsprincipen i 2 kap. TF. Utredningens förslag innebär att dataskyddsförordningen och dataskyddslagen inte ska tillämpas i den utsträckning det skulle strida mot bestämmelserna om tryck- och yttrandefrihet i tryckfrihetsförordningen eller yttrandefrihetsgrundlagen. Genom att begränsningen till bestämmelser om tryck- och yttrandefrihet tas bort kan det klargöras att bestämmelsen även avser bestämmelserna om allmänna handlingars offentlighet i 2 kap. TF.

Regeringen föreslår alltså att det införs en bestämmelse i dataskyddslagen med innebörden att dataskyddsförordningen och dataskyddslagen inte ska tillämpas i den utsträckning det skulle strida mot tryckfrihetsförordningen eller yttrandefrihetsgrundlagen.

7.2 Undantag utanför det grundlagsskyddade området

Regeringens förslag: Bestämmelserna i EU:s dataskyddsförordning och dataskyddslagen om principer, den registrerades rättigheter, vissa skyldigheter för den personuppgiftsansvarige och personuppgiftsbiträdet, uppförandekoder och certifiering samt överföring av personuppgifter till tredjeländer eller internationella organisationer ska inte tillämpas vid behandling av personuppgifter som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande utanför tryckfrihetsförordningens och yttrandefrihetsgrundlagens tillämpningsområde. Bestämmelserna om syfte, tillämpningsområde och definitioner samt bestämmelser om säkerhet för personuppgifter, tillsyn, rättsmedel, ansvar och sanktioner ska dock tillämpas även i dessa fall.

Utredningens förslag överensstämmer i sak med regeringens.

Remissinstanserna: Det stora flertalet remissinstanser tillstyrker förslaget eller har inga synpunkter på det. *Sveriges Radio AB* delar utredningens bedömning och anför att rätten att informera, utöva kritik samt väcka debatt om samhällsfrågor är av central betydelse även utanför det grundlagsskyddade området. *Stiftelsen Svenska Filminstitutet*, som ser positivt på utredningens förslag, understryker vikten av att filmarbetare inte hämmas i sin skapandeprocess av en omfattande dataskyddsreglering. Enligt *Vetenskapsrådet* riskerar rådande oklarhet om innebörden av begreppet akademiskt skapande leda till tolkningsproblem och oönskade konsekvenser innan praxis hunnit utvecklats på området.

Skälen för regeringens förslag: I 7 § andra stycket PUL görs undantag från stora delar av lagens bestämmelser vid personuppgiftsbehandling som inte omfattas av tryckfrihetsförordningen eller yttrandefrihets-

grundlagen, men som sker uteslutande för journalistiska ändamål eller konstnärligt eller litterärt skapande. Undantaget har införts med stöd av artikel 9 i dataskyddsdirektivet (se avsnitt 7.1) och innebär i praktiken att bara de bestämmelser i lagen som rör tillsyn och säkerhet vid behandling ska tillämpas i sådan verksamhet. Undantagsbestämmelsen i 7 § andra stycket PUL har ansetts tillämplig exempelvis på journalistisk verksamhet utanför det grundlagsskyddade området på internet som resulterar i yttranden som endast sprids där och även för viss kommunikation som inte bedrivs av yrkesverksamma journalister (prop. 1997/98:44 s. 52–53 och NJA 2001 s. 409).

Genom artikel 85.2 i förordningen åläggs medlemsstaterna att göra vissa undantag från förordningen för behandling som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande. Undantag får dock bara göras om de är nödvändiga för att förena rätten till integritet med yttrande- och informationsfriheten. I skäl 153 i dataskyddsförordningen anges att undantag särskilt bör gälla vid personuppgiftsbehandling inom det audiovisuella området och i nyhetsarkiv samt pressbibliotek.

Begreppet akademiskt skapande är nytt och definieras inte närmare vare sig i skäl eller i artikeltext. Som utredningen påpekar torde begreppet dock inte omfatta forskning, eftersom personuppgiftsbehandling för forskningsändamål är särreglerad på annat sätt i förordningen. Möjligen skulle behandling i samband med själva färdigställandet och spridningen av texter med vetenskapligt innehåll kunna avses. Det är dock vanskligt att uttala sig närmare om begreppets innebörd i nuläget. Innebörden av begreppet kommer i stället att få utvecklas i praxis.

Som konstateras i avsnitt 7.1 innebär artikel 85.2 att möjligheterna till undantag från förordningen är något större än de som i dag gäller enligt dataskyddsdirektivet. Regeringen delar därför utredningens bedömning att det även fortsättningsvis finns möjlighet att ha ett undantag av det slag som finns i 7 § andra stycket PUL. Det kan konstateras att betydelsen av opinionsbildning genom alternativa kanaler såsom sociala medier, bloggar och liknande har ökat dramatiskt under senare år. Detta medför att skälen för ett undantag utanför tryckfrihetsförordningens och yttrandefrihetsgrundlagens tillämpningsområde inte har minskat och inte heller kan förutses göra det framöver. I likhet med utredningen anser regeringen därför att det bör införas ett undantag för behandling av personuppgifter som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande i den utsträckning som förordningen tillåter det.

Enligt artikel 85.2 är det inte möjligt att införa undantag beträffande kapitel I om syfte, tillämpningsområde och definitioner, kapitel VIII om rättsmedel, ansvar och sanktioner samt kapitel X och XI som innehåller genomförande- och slutbestämmelser. Förordningens bestämmelser om särskilda behandlingssituationer i kapitel IX torde knappast bli tillämpliga för den behandling som avses här, varför de inte behöver undantas uttryckligen. I likhet med vad som gäller enligt 7 § andra stycket PUL, bör undantag inte heller göras från de bestämmelser som rör säkerhet för personuppgifter och tillsyn. Sammantaget innebär detta att undantaget bör omfatta bestämmelserna i artiklarna 5–30 och 35–50 i dataskydds-

förordningen, liksom de delar av dataskyddslagen som har stöd i de aktuella bestämmelserna.

8 Rättslig grund för behandling av personuppgifter

8.1 Laglig behandling

Den europeiska dataskyddsregleringen utgår från att varje behandling av personuppgifter måste vila på en rättslig grund. I dataskyddsförordningen räknas dessa rättsliga grunder upp i artikel 6.1. Behandling är enligt denna bestämmelse laglig endast om och i den mån som åtminstone ett av följande villkor är uppfyllt:

a) Den registrerade har lämnat sitt samtycke till att dennes personuppgifter behandlas för ett eller flera specifika ändamål.

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.

c) Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige.

d) Behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person.

e) Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.

f) Behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter, särskilt när den registrerade är ett barn.

Bestämmelsen motsvarar i stora drag artikel 7 i dataskyddsdirektivet, som har genomförts i svensk rätt genom 10 § PUL. Den största skillnaden är att det enligt förordningen inte är tillåtet för myndigheter att, när de fullgör sina uppgifter, behandla personuppgifter med stöd av den rättsliga grund som utgår från en avvägning mellan den ansvariges berättigade intressen och den registrerades rättigheter och intressen (artikel 6.1 f). I detta sammanhang kan nämnas att flera remissinstanser efterfrågar en definition av begreppet myndighet. Artikel 29-arbetsgruppen för skydd av personuppgifter anser att detta begrepp bör definieras i nationell lagstiftning (Riktlinjer om dataskyddsombud, WP 243 rev.01). Regeringen bedömer mot den bakgrunden att det är regeringsformens terminologi som i Sverige bör vara utgångspunkten vid tolkningen av begreppet myndighet i dataskyddsförordningen. Enligt denna terminologi är samtliga statliga och kommunala organ myndigheter, med undantag av riksdagen, kommun- och landstingsfullmäktige.

Organ som är organiserade i privaträttsliga former, t.ex. kommunala och statliga bolag, är inte myndigheter, även om de utövar offentlig makt.

Uppräkningen i artikel 6.1 är uttömmande. Om ingen av de grunder som anges där är tillämplig är behandlingen inte laglig och får därmed inte utföras. Detta gäller all behandling av personuppgifter, även sådan ostrukturerad behandling som i dag kan ske utan stöd av rättslig grund enligt missbruksregeln i 5 a § PUL. De rättsliga grunderna är i viss mån överlappande. Flera rättsliga grunder kan därför vara tillämpliga avseende en och samma behandling.

För att en behandling av personuppgifter ska vara tillåten enligt artikel 6.1 b–f måste den vara nödvändig i förhållande till den rättsliga grunden, t.ex. nödvändig för att utföra en uppgift av allmänt intresse. Enligt Svenska Akademiens Ordbok betyder det svenska ordet nödvändig att någonting absolut fordras eller inte kan underlåtas. Det unionsrättsliga begreppet har dock inte denna strikta innebörd. Nödvändighetsrekvisitet i artikel 7 i dataskyddsdirektivet har t.ex. inte ansetts utgöra ett krav på att det ska vara omöjligt att utföra en uppgift av allmänt intresse utan att behandlingsåtgärden vidtas. Detta synsätt kommer till uttryck i EU-domstolens dom i målet Huber mot Tyskland, som rörde tolkningen av motsvarande nödvändighetsrekvisit i artikel 7 e i direktivet (C-524/06, EU:C:2008:724). EU-domstolen uttalade att en myndighets förande av ett centralt register över uppgifter som redan fanns i regionala register är nödvändigt om det bidrar till att effektivisera tillämpningen av relevanta bestämmelser. Domen bör kunna utgöra stöd även vid tolkningen av dataskyddsförordningen. På motsvarande sätt bör det i dagsläget mer eller mindre regelmässigt anses vara nödvändigt att använda tekniska hjälpmedel och därmed behandla personuppgifter på automatisk väg, eftersom en manuell informationshantering inte utgör ett realistiskt alternativ för vare sig myndigheter eller företag.

Utöver det grundläggande kravet på att all behandling måste vara laglig, i betydelsen att någon av de rättsliga grunder som anges i artikel 6.1 i dataskyddsförordningen är tillämplig, omgärdas varje behandling av personuppgifter också av andra krav. Principerna för behandling av personuppgifter, dvs. vilka allmänna krav som gäller för all personuppgiftsbehandling, anges i artikel 5.1 i dataskyddsförordningen. Den bestämmelsen motsvarar i stora drag artikel 6 i dataskyddsdirektivet, som har genomförts i svensk rätt genom 9 § PUL.

Den första principen som läggs fast i artikel 5.1 är att personuppgifter ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade (led a). Principen om laglighet kan sägas utgöra en hänvisning till de rättsliga grunderna i artikel 6.1. Såvitt avser principen om korrekthet kan det vid en jämförelse med andra språkversioner ifrågasättas om den svenska termen korrekt motsvarar avsikten med bestämmelsen. I den danska språkversionen anges i stället att uppgifterna ska behandlas *rimeligt*. På motsvarande sätt används i den engelska språkversionen termen *fairly*, vilket betyder rättvist, skäligt eller rimligt. I den franska språkversionen används termen *loyale*, vilken har motsvarande betydelse som engelskans *fairly*. I den tyska språkversionen används uttrycket *Treu und Glauben*, vilket brukar översättas med god tro eller tro och heder. Alla dessa termer indikerar enligt regeringens mening, tydligare än den svenska termen korrekt, att en intresseavvägning ska

göras. I det enskilda fallet kan det således t.ex. vara oförenligt med principen om korrekthet att vidta en viss behandlingsåtgärd, även om denna i och för sig skulle kunna anses vara rättsligt grundad enligt artikel 6, nämligen om behandlingen är oskälig i förhållande till den registrerade.

I artikel 5.1 anges vidare att personuppgifterna ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och att de inte senare får behandlas på ett sätt som är oförenligt med dessa ändamål (led b). Principen om att ändamålen ska vara berättigade utgör i likhet med principen om laglighet en direkt koppling till de rättsliga grunderna i artikel 6.1. Ett ändamål som inte är berättigat i förhållande till den tillämpliga rättsliga grunden är således inte förenligt med artikel 5. Ett tydligt angivet ändamål är för övrigt som regel en förutsättning för att man ska kunna bedöma om en viss behandling är laglig, dvs. om den är nödvändig i något av de sammanhang som räknas upp i artikel 6.1 b–f.

Kopplingen mellan den rättsliga grunden och kravet på särskilda, uttryckligt angivna och berättigade ändamål förstärks genom dataskyddsförordningen, där det av artikel 6.3 andra stycket framgår att syftet med behandlingen, i fråga om behandling som grundar sig på en rättslig förpliktelse, ska framgå av förpliktelsen. Vad gäller behandling som sker i myndighetsutövning och för att utföra uppgifter av allmänt intresse anges i stället att syftet med behandlingen ska vara nödvändigt för att utföra uppgiften eller myndighetsutövningen.

Vidare ska uppgifterna enligt artikel 5.1 bl.a. vara adekvata och korrekta (*accurate*) och får inte förvaras under en längre tid än vad som är nödvändigt (leden c, d och e). Uppgifterna måste också behandlas på ett sätt som säkerställer lämplig säkerhet (led f).

Förordningen ställer inte något krav på att de särskilda ändamålen ska vara fastställda i författning, men det finns heller ingenting som hindrar att detta görs, förutsatt att bestämmelserna uppfyller ett mål av allmänt intresse och är proportionella mot det legitima mål som eftersträvas (artikel 6.3 andra stycket). Oavsett om ändamålen fastställts i författning eller inte är det dock alltid den personuppgiftsansvarige som ansvarar för, och ska kunna visa att, principerna i artikel 5 efterlevs (artikel 5.2).

Artiklarna 5 och 6 i dataskyddsförordningen är grundläggande och kumulativa. Dels måste någon av de rättsliga grunder som anges i artikel 6.1 vara tillämplig, dels måste samtliga principer i artikel 5.1 följas.

8.2 Grunden för behandlingen ska ha stöd i rättsordningen

Regeringens bedömning: Kravet i EU:s dataskyddsförordning på att den grund för behandling som avses i artikel 6.1 c och e ska vara fastställd i enlighet med unionsrätten eller den nationella rätten innebär inte ett krav på att själva behandlingen av personuppgifter måste regleras. Det är i stället den rättsliga förpliktelsen, uppgiften av allmänt intresse respektive myndighetsutövningen som ska ha stöd i rättsordningen.

Den rättsliga förpliktelsen, uppgiften av allmänt intresse respektive myndighetsutövningen är fastställd i enlighet med svensk rätt, om den följer av författning eller beslut som har meddelats i enlighet med regeringsformens bestämmelser. Som en följd av den svenska arbetsmarknadsmodellen kan rättsliga förpliktelser och uppgifter av allmänt intresse även följa av kollektivavtal.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Nästan alla remissinstanser instämmer i utredningens bedömning eller har inga synpunkter på denna. *Srf konsulternas förbund* ifrågasätter bedömningen i fråga om kollektivavtal och påpekar att avtalen inte är allmänt tillgängliga. Även *Datainspektionen* och *dataskydd.net* ifrågasätter utredningens bedömning i fråga om kollektivavtal. Flera remissinstanser, bl.a. *Arbetsgivarverket*, *Karlskrona kommun*, *Landsorganisationen i Sverige* och *Collectum*, uttrycker å andra sidan sitt stöd för denna bedömning. Datainspektionen menar att det finns risk för att behandling av personuppgifter av vikt för samhällets funktioner inte kan utföras, om det inte säkerställs att särskild nationell lagstiftning införs där behov finns. Vidare menar Datainspektionen att de personuppgiftsansvariga som ska tillämpa förordningen måste göra en bedömning av om den författning som kan utgöra rättslig grund för behandlingen uppfyller kraven bl.a. på tydlighet, precisering och förutsägbarhet i skäl 41 samt kraven på proportionalitet i artikel 6.3 andra stycket sista meningen.

Skälen för regeringens bedömning

Vad ska fastställas i unionsrätten eller nationell rätt?

Som nämns i avsnitt 8.1 får behandling av personuppgifter bara ske under de omständigheter som särskilt anges i unionsrätten eller i den nationella rätten. Detta rättsliga stöd ges direkt i dataskyddsförordningen såvitt gäller behandling som sker på grundval av den registrerades samtycke, för att fullgöra ett avtal, för att skydda en fysisk persons grundläggande intressen samt för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen (artikel 6.1 a, b, d och f). Eftersom dessa bestämmelser inte föranleder några nationella författningsåtgärder behandlas de inte här (se dock avsnitt 9 angående barns samtycke).

När det gäller behandling som är nödvändig för att fullgöra en rättslig förpliktelse (artikel 6.1 c), som ett led i myndighetsutövning eller för att

utföra en uppgift av allmänt intresse (artikel 6.1 e) måste det emellertid även finnas ett annat stöd i rättsordningen än det som ges i dataskyddsförordningen. I artikel 6.3 första stycket i dataskyddsförordningen anges det nämligen att den grund för behandlingen som avses i artikel 6.1 c och e ska fastställas i enlighet med unionsrätten eller en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av. I skäl 45 till dataskyddsförordningen anges att förordningen inte medför något krav på en särskild lag för varje enskild behandling, utan att det kan räcka med en lag som grund för flera behandlingar som bygger på en rättslig förpliktelse som åvilar den personuppgiftsansvarige eller om behandlingen krävs för att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning.

Av ordalydelsen i artikel 6.3 första stycket framgår att det som ska fastställas i unionsrätten eller i nationell rätt är den grund för behandlingen som avses i artikel 6.1 c och e. Det krävs således inte en reglering i unionsrätten eller i nationell rätt av den personuppgiftsbehandling som ska ske med stöd av dessa rättsliga grunder. Det som måste ha stöd i rättsordningen är i stället den rättsliga förpliktelsen respektive uppgiften av allmänt intresse eller rätten att utöva myndighet.

Vad menas med att grunden för behandlingen ska vara fastställd?

Kravet i artikel 6.3 första stycket på att grunden för behandlingen i vissa fall ska fastställas utgör ett villkor som måste vara uppfyllt för att personuppgiftsansvariga ska kunna åberopa de rättsliga grunder som avses i artikel 6.1 c och e. Rättsliga förpliktelser, uppgifter av allmänt intresse och myndighetsutövning som inte är fastställda i enlighet med unionsrätten eller medlemsstatens nationella rätt kan därmed inte läggas till grund för behandling av personuppgifter.

Något motsvarande krav på att grunden för behandlingen ska vara fastställd finns inte i dataskyddsdirektivet. Det har därför t.ex. ansetts möjligt att med stöd av 10 § d PUL utföra behandling av personuppgifter som är nödvändig för att utföra en arbetsuppgift av allmänt intresse, även om uppgiften inte är fastställd i författning eller liknande.

Det bör emellertid betonas att dataskyddsförordningens krav på att grunden för behandlingen ska vara fastställd inte utgör någon nyhet när det gäller svenska myndigheters behandling av personuppgifter. Legalitetsprincipen är en av de principer som kännetecknar Sverige som rättsstat. Principen är grundlagsfäst genom 1 kap. 1 § RF, som anger att den offentliga makten utövas under lagarna. Med uttrycket lagarna avses inte bara sådana föreskrifter som riksdagen har beslutat, utan även andra författningar och t.ex. sedvanerätt (prop. 1973:90 s. 397 och KU 1973:26 s. 59). Legalitetsprincipen innebär alltså att myndigheternas maktutövning i vidsträckt mening, även i den mån denna förutsätter behandling av personuppgifter, måste ha stöd i någon av de källor som tillsammans bildar rättsordningen.

Datainspektionen menar att det finns risk för att behandling av personuppgifter av vikt för samhällets funktioner inte kan utföras, om det inte säkerställs att särskild nationell lagstiftning införs där behov finns. Regeringen bedömer emellertid att denna risk är mycket liten, eftersom det inte torde förekomma någon offentlig verksamhet i Sverige av vikt

för samhällets funktioner som saknar stöd i författning eller beslut som har meddelats i enlighet med regeringsformens bestämmelser.

Vidare menar Datainspektionen att de personuppgiftsansvariga som ska tillämpa förordningen måste göra en bedömning av om den författning som kan utgöra rättslig grund för behandlingen uppfyller kraven på proportionalitet i artikel 6.3 andra stycket sista meningen. Regeringen kan konstatera att den bestämmelsen anger att unionsrätten eller medlemsstaternas nationella rätt ska uppfylla ett mål av allmänt intresse och vara proportionell mot det legitima mål som eftersträvas. Detta motsvarar det krav som Europakonventionen ställer på lagstiftaren i en rättsstat. Genom lagen (1994:1219) om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna har Europakonventionen inkorporerats i svensk rätt. Vidare gäller enligt 2 kap. 19 § RF att lagar och andra föreskrifter inte får meddelas i strid med Sveriges åtaganden enligt Europakonventionen. Det bör därför vara mycket ovanligt att svensk rätt inte uppfyller Europakonventionens krav. Mot denna bakgrund bör utgångspunkten vara att även dataskyddsförordningens motsvarande krav är uppfyllt i fråga om de rättsliga förpliktelser, uppgifter av allmänt intresse och den myndighetsutövning som fastställs i enlighet med svensk rätt. Den personuppgiftsansvarige behöver därmed inte göra någon proportionalitetsbedömning avseende regleringen av den rättsliga grunden för behandlingen, utan kan utgå från att svensk rätt uppfyller detta krav. Däremot måste behandlingen vara nödvändig i förhållande till den rättsliga grunden och följa de grundläggande principerna i artikel 5. Dessutom ankommer det på varje svensk myndighet att i all verksamhet iaktta proportionalitetskravet. Detta krav kommer numera även till uttryck i 5 § i den nya förvaltningslagen, där det anges att en åtgärd aldrig får vara mer långtgående än vad som behövs och att den får vidtas endast om det avsedda resultatet står i rimligt förhållande till de olägenheter som kan antas uppstå för den som åtgärden riktas mot.

Av skäl 41 till förordningen framgår att den rättsliga grunden bör vara tydlig och precis och dess tillämpning förutsägbar för dem som omfattas av den, i enlighet med rättspraxis vid Europeiska unionens domstol och Europeiska domstolen för de mänskliga rättigheterna. Även detta är ett uttryck för legalitetsprincipen och utgör således inte någon nyhet inom den svenska offentliga förvaltningen. Vilken grad av tydlighet och precision som krävs i fråga om den rättsliga grunden för att en viss behandling av personuppgifter ska anses vara nödvändig måste enligt regeringens mening bedömas från fall till fall, utifrån behandlingens och verksamhetens karaktär. Det torde stå klart att en behandling av personuppgifter som inte utgör någon egentlig kränkning av den personliga integriteten, såsom när det gäller behandling av elevers namn i reguljär skolverksamhet, kan ske med stöd av en rättslig grund som är allmänt hållen. Ett mer kännbart intrång, t.ex. behandling av känsliga personuppgifter inom hälso- och sjukvården, kräver att den rättsliga grunden är mer preciserad och därmed gör intrånget förutsebart. Om intrånget är betydande och innebär övervakning eller kartläggning av den enskildes personliga förhållanden krävs dessutom särskilt lagstöd enligt 2 kap. 6 och 20 §§ RF.

Hur fastställs en rättslig grund i enlighet med svensk rätt?

Grunden för behandlingen ska enligt artikel 6.3 första stycket i dataskyddsförordningen fastställas i enlighet med unionsrätten eller en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av. Med detta avses inte att den rättsliga grunden nödvändigtvis måste fastställas i eller i enlighet med en av riksdagen beslutad lag. Däremot måste grunden vara fastställd i laga ordning, på ett konstitutionellt korrekt sätt.

I Sverige följer det av grundlag att den offentliga makten utövas under lagarna. De grundläggande bestämmelserna om hur normgivningen går till finns i 8 kap. RF. Föreskrifter ska meddelas av riksdagen genom lag bl.a. om föreskrifterna avser förhållandet mellan enskilda och det allmänna under förutsättning att föreskrifterna gäller skyldigheter för enskilda eller i övrigt avser ingrepp i enskildas personliga och ekonomiska förhållanden. Regeringen får dock, efter bemyndigande från riksdagen, meddela sådana föreskrifter i en förordning. Normgivningskompetensen kan även vidaredelegeras till en myndighet eller en kommun, som därmed bemyndigas att meddela föreskrifter på ett visst område. När det gäller föreskrifter som är gynnande för den enskilde får regeringen, inom ramen för sin restkompetens, meddela föreskrifter om åtgärder utan stöd av ett bemyndigande från riksdagen.

Av 1 kap. 6 § RF framgår att regeringen styr riket. Under regeringen lyder de statliga förvaltningsmyndigheter som inte är myndigheter under riksdagen. Regeringen styr dessa myndigheter genom regeringsbeslut och genom att med stöd av restkompetensen meddela föreskrifter. Det kommunala självstyret innebär att fullmäktige har visst utrymme att styra de kommunala myndigheternas verksamhet genom reglementen.

Enligt lagen (1994:1500) med anledning av Sveriges anslutning till Europeiska unionen gäller EU-rättsakter här i landet med den verkan som följer av EU-fördragen. Detta innebär att även unionsrätten har stöd i svensk lag, t.ex. i fråga om förpliktelser, myndighetsutövning och uppgifter av allmänt intresse som följer av direkt tillämpliga EU-förordningar eller som meddelas med stöd av sådana förordningar.

Den svenska arbetsmarknadsmodellen innebär att arbetsmarknadens parter i stor utsträckning reglerar arbets- och anställningsvillkor genom kollektivavtal. Kollektivavtalen innehåller en rad bestämmelser som arbetsmarknadens parter och medlemmarna i de avtalsslutande organisationerna är skyldiga att följa, t.ex. om föräldratillägg, semesterlön, övertidsersättning och ersättning för läkarbesök och läkemedel. Överträdelser av bestämmelserna kan föranleda skadeståndsansvar. Kollektivavtalen har även betydelse för tredje man eftersom de ska tillämpas på samma sätt i förhållande till alla arbetstagare och således även i förhållande till oorganiserade arbetstagare och arbetstagare som är medlemmar i en annan arbetstagarorganisation än den som avtalet slutits med.

Reglering i kollektivavtal har i Europadomstolens praxis ansetts i sig förenlig med kravet enligt Europakonventionen att åtgärder med rättighetsbegränsande effekter ska ha stöd i lag (jfr Europadomstolens dom i målet Evaldsson mot Sverige, nr 75252/01, dom den 13 februari 2007). Denna praxis talar för att samma princip bör gälla vid tillämpningen av EU-lagstiftning som rör fri- och rättigheter, såsom dataskyddsförord-

ningen. Eftersom kollektivavtal utgör en del av den svenska rättsordningen bör således grunden för behandlingen av personuppgifter kunna anses vara fastställd i enlighet med svensk rätt om den följer av kollektivavtal. Regeringen delar mot den bakgrunden, i likhet med bl.a. *Arbetsgivarverket* och *Landsorganisationen i Sverige*, utredningens bedömning.

Med anledning av *Srf konsulternas förbunds* synpunkter vill regeringen betona att för att ett kollektivavtal ska kunna läggas till grund för behandling av personuppgifter så måste det vara tillgängligt för den registrerade. I annat fall är det grundläggande legalitetskravet i dataskyddsförordningen inte uppfyllt.

Sammanfattningsvis konstaterar regeringen att en rättslig grund är fastställd i enlighet med svensk rätt om den följer av författning eller beslut som meddelats i enlighet med regeringsformens bestämmelser. Som en följd av den svenska arbetsmarknadsmodellen kan en rättslig grund även följa av kollektivavtal.

8.3 Behandling för att uppfylla en rättslig förpliktelse

Regeringens förslag: Personuppgifter får behandlas om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna fullgöra en rättslig förpliktelse som följer av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning.

Utredningens förslag överensstämmer i sak med regeringens.

Remissinstanserna: Nästan alla remissinstanser tillstyrker förslaget eller har inga synpunkter på det. *Datainspektionen* anser att det i bestämmelsen ska anges att kraven i artikel 6.3 måste följas. Några remissinstanser, bl.a. *Skatteverket* och *Collectum*, efterfrågar ett tydliggörande kring hur förordningens bestämmelse om att syftet med behandlingen ska fastställas i den rättsliga grunden ska tolkas och tillämpas i praktiken.

Skälen för regeringens förslag

Begreppet rättslig förpliktelse

Bestämmelsen i artikel 6.1 c i dataskyddsförordningen överensstämmer i sak med artikel 7 c i dataskyddsdirektivet. Enligt båda bestämmelserna får personuppgifter behandlas om behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige. Enligt regeringens bedömning bör utgångspunkten vara att begreppet rättslig förpliktelse i de båda rättsakterna ska tolkas och tillämpas på samma sätt. Vägledning bör därför kunna hämtas från praxis som utvecklats i anslutning till dataskyddsdirektivet och personuppgiftslagen.

I första hand torde offentligrättsliga förpliktelser omfattas av begreppet rättslig förpliktelse. Det finns dock även i civilrättsliga författningar bestämmelser som i sig utgör eller kan medföra rättsliga skyldigheter, t.ex. inom arbetsrätten. Rent språkligt omfattar begreppet rättslig för-

pliktelse även sådana skyldigheter som har lagts fast i ett avtal. Förpliktelser som följer av avtal där den registrerade själv är part utgör emellertid en separat rättslig grund för personuppgiftsbehandling enligt både dataskyddsdirektivet och dataskyddsförordningen, nämligen led b i respektive artikel. Detta talar för att de rättsliga förpliktelser som avses i led c är av ett annat slag, även om förpliktelser som följer av vissa lagreglerade avtal, t.ex. försäkringsavtal av betydelse för andra än parterna eller gynnande tredjemansavtal, skulle kunna omfattas av bestämmelsen.

Rättsliga förpliktelser har stöd i rättsordningen

Som nämns i avsnitt 8.2 följer det av grundlag att den offentliga makten utövas under lagarna. Förpliktelser som åligger enskilda eller kommuner kan regleras direkt i lag, i förordningar eller andra föreskrifter. Förpliktelser kan också fastställas i domar eller myndighetsbeslut som meddelats med stöd av lag eller andra föreskrifter. Som en följd av den svenska arbetsmarknadsmodellen kan rättsliga förpliktelser även anges i kollektivavtal. Sådana avtal omfattas inte av artikel 6.1 b, eftersom den registrerade inte själv är part.

Även domstolar och förvaltningsmyndigheter kan, vid sidan av sina uppgifter och uppdrag, sägas ha rättsliga förpliktelser. Domstolar och förvaltningsmyndigheter har t.ex. när det gäller personaladministration författningsreglerade förpliktelser som i sig kräver personuppgiftsbehandling. Vidare kan en myndighets uppdrag enligt instruktionen till myndigheten eller ett regleringsbrev i vissa fall utgöra en i enlighet med nationell rätt fastställd rättslig förpliktelse i dataskyddsförordningens mening, t.ex. om myndigheten ges i uppdrag att föra ett visst register. I normalfallet torde dock myndighetens uppdrag i första hand utgöra en rättslig grund för behandling av personuppgifter med stöd av artikel 6.1 e i dataskyddsförordningen, dvs. på grundval av att uppdraget avser en uppgift av allmänt intresse, se avsnitt 8.4.

Syftet med behandlingen ska framgå av förpliktelsen

Enligt artikel 6.3 andra stycket första meningen i dataskyddsförordningen ska syftet med behandlingen, då denna grundar sig på en rättslig förpliktelse, fastställas i den rättsliga grunden. Några remissinstanser, bl.a. *Skatteverket* och *Collectum*, efterfrågar ett tydliggörande av hur bestämmelsen ska tolkas och tillämpas i praktiken. Kravet torde innebära att en förpliktelse inte kan läggas till grund för behandling av personuppgifter om syftet med behandlingen inte framgår. Det ska alltså vara möjligt för såväl den personuppgiftsansvarige som den registrerade att förstå varför behandlingen av personuppgifter ska ske. Detta kan exempelvis ske genom en författning som anger att en näringsidkare i en viss situation är skyldig att lämna uppgifter till en myndighet eller en domstol.

Behov av förtydligande i nationell rätt

Regeringen gör bedömningen att det i och för sig inte behövs någon ytterligare nationell reglering på generell nivå för att sådan behandling av personuppgifter som är nödvändig för att uppfylla en rättslig förpliktelse

ska kunna ske med stöd av den rättsliga grunden i artikel 6.1 c i dataskyddsförordningen. Detta gäller oavsett om den personuppgiftsansvarige är en myndighet eller ett privaträttsligt organ. Regeringen anser dock, i likhet med utredningen, att det finns anledning att ta in en bestämmelse i dataskyddslagen som tydliggör att en förpliktelse utgör en rättslig grund för behandling av personuppgifter om förpliktelsen följer av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning. Detta är enligt skäl 8 till dataskyddsförordningen förenligt med unionsrätten, även om åtgärden kan sägas utgöra ett införlivande av en direkt tillämplig förordningsbestämmelse.

Datainspektionen anser att det i bestämmelsen ska anges att kraven i artikel 6.3 andra stycket i dataskyddsförordningen måste följas och anför att det måste vara tydligt för den enskilde tillämparen att behandlingen av personuppgifter i varje enskilt fall ska uppfylla ett mål av allmänt intresse och vara proportionell mot det legitima mål som eftersträvas. Som regeringen utvecklar i avsnitt 8.2 måste dock kravet i artikel 6.3 andra stycket sista meningen på att unionsrätten eller medlemsstatens nationella rätt ska uppfylla ett mål av allmänt intresse och vara proportionell mot det legitima mål som eftersträvas i första hand anses riktat till lagstiftaren och andra som har befogenhet att fastställa rättsliga förpliktelser och inte till personuppgiftsansvariga eller personuppgiftsbiträden. Det finns därför inte skäl att föra in en hänvisning till dessa krav i dataskyddslagen.

8.4 Behandling för att utföra uppgifter av allmänt intresse

Regeringens förslag: Personuppgifter får behandlas om behandlingen är nödvändig för att utföra en uppgift av allmänt intresse som följer av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning.

Utredningens förslag överensstämmer i huvudsak med regeringens. Utredningen föreslår att det i bestämmelsen ska anges att behandlingen ska vara nödvändig för att den personuppgiftsansvarige ska kunna utföra en uppgift av allmänt intresse.

Remissinstanserna: Nästan alla remissinstanser tillstyrker förslaget eller har inga synpunkter på det. *Pensionsmyndigheten* och *Statens servicecenter* anser att den föreslagna regleringen tillsammans med principerna i artikel 5 förtydligar det som redan gäller. *Malmö kommun* och *Piteå kommun* anser att förslaget underlättar förståelsen av dataskyddslagstiftningen. *Datainspektionen* anser att det i bestämmelsen ska anges att kraven i artikel 6.3 andra stycket måste följas. Vidare anför Datainspektionen att det kan utgöra ett allmänt intresse att myndigheter även kan vidta administrativa åtgärder, men att det är svårt att se att dessa alltid kan anses vara fastställda i enlighet med unionsrätten eller den nationella rätten. *Åklagarmyndigheten* anser att det behövs ett tydligt stöd för behandling av personuppgifter för ändamål som statistik och

uppföljning av verksamheten. *Tjänstemännens centralorganisation* anser att det bör klargöras att arbetsmarknadsparternas framtagande och behandling av lönestatistik m.m. är att betrakta som en uppgift av allmänt intresse. *Stiftelsen Svenska Filminstitutet* efterfrågar ledning för tolkningen av begreppen offentligt organ samt sådant privat organ som utför uppgifter av allmänt intresse, som omnämns i förordningens artikel 86. *Svenska kyrkan* ser en konflikt mellan dataskyddsförordningen och kravet på handlingsoffentlighet gentemot envar i 11 § lagen (1998:1591) om Svenska kyrkan. *Dataskydd.net* anser att bestämmelsen är onödig.

Skälen för regeringens förslag

Begreppet uppgift av allmänt intresse

Enligt artikel 6.1 e i dataskyddsförordningen får personuppgifter behandlas om behandlingen är nödvändig för att utföra en uppgift av allmänt intresse. Flera remissinstanser efterlyser vägledning rörande begreppets innebörd. Rent språkligt kan begreppet uppgift av allmänt intresse antas avse något som är av intresse för eller berör många människor på ett bredare plan, i motsats till ett särintresse eller ett enskilt intresse. Av skäl 45 till förordningen följer att allmänintresset inbegriper hälso- och sjukvårdsändamål, folkhälsa, socialt skydd och förvaltning av hälso- och sjukvårdstjänster. Det kan vidare konstateras att begreppet förekommer i motsvarande bestämmelser i dataskyddsdirektivet (artikel 7 e) och personuppgiftslagen (10 § d) och ledning kan hämtas från hur begreppet tolkats enligt dessa bestämmelser.

Vid tillämpningen av personuppgiftslagen har den behandling av personuppgifter som är nödvändig i t.ex. myndigheternas verksamhet i vissa fall ansetts vara tillåten efter en intresseavvägning enligt 10 § f PUL. Den motsvarande bestämmelsen i dataskyddsförordningen, artikel 6.1 f, ska dock inte gälla för behandling som utförs av offentliga myndigheter när de utför sina uppgifter. Myndigheternas utrymme för att grunda behandling på samtycke från den registrerade är också alltjämt begränsat, i vart fall i sådana situationer där det är osannolikt att ett samtycke lämnas frivilligt (skäl 43). För att myndigheternas verksamhet ska kunna fungera även i fortsättningen anser regeringen att begreppet uppgift av allmänt intresse måste ges en vid betydelse.

I förhållande till den privata sektorn innebär dataskyddsförordningen en väsentlig förändring på så sätt att det inte längre är självklart att en personuppgiftsansvarig inom den sektorn som utför en uppgift av allmänt intresse kan utföra nödvändig behandling av personuppgifter på den grunden. Genom kravet på att grunden för behandlingen ska fastställas i enlighet med unionsrätten eller den nationella rätten begränsas nämligen tillämpningsområdet för artikel 6.1 e. Det räcker inte att en behandling av personuppgifter är nödvändig för att utföra en uppgift av allmänt intresse – uppgiften måste också vara fastställd i enlighet med gällande rätt. När det gäller *Tjänstemännens centralorganisations* synpunkt om arbetsmarknadsparternas framtagande och behandling av lönestatistik m.m., kan konstateras att Datalagskommittén ansåg att denna uppgift var av allmänt intresse enligt personuppgiftslagen (SOU 1997:39 s. 305). Det finns inte anledning att göra någon annan bedömning enligt dataskydds-

förordningen. För att personuppgifter ska kunna behandlas på denna rättsliga grund krävs emellertid också att uppgiften är fastställd i enlighet med svensk rätt och att behandlingen är nödvändig.

När det däremot gäller svenska myndigheters behandling av personuppgifter innebär dataskyddsförordningens krav på att grunden för behandlingen ska vara fastställd inte någon egentlig förändring. Som utvecklas i avsnitt 8.2 innebär legalitetsprincipen nämligen att myndigheternas verksamhet redan i dag måste vara fastställd enligt svensk rätt.

Enligt artikel 6.3 andra stycket första meningen i dataskyddsförordningen ska syftet med behandlingen, i fråga om behandling enligt punkt 1 e, vara nödvändigt för att utföra en uppgift av allmänt intresse. Till skillnad mot vad som gäller avseende grunden rättslig förpliktelse behöver ändamålet således inte framgå. Ändamålet med varje enskild behandling måste dock vara nödvändigt för att utföra den fastställda uppgiften. Bestämmelsen uttrycker det samband som måste finnas mellan behandlingen och den fastställda uppgiften och riktar sig till den som bestämmer de särskilda ändamålen för behandlingen, vilket i normalfallet är den personuppgiftsansvarige men i vissa fall även kan vara lagstiftaren. Detta krav på samband framgår även av artikel 5.1 b, där det anges att de särskilda ändamålen ska vara berättigade.

Myndigheters verksamhet är av allmänt intresse

Alla uppgifter som riksdag eller regering gett i uppdrag åt statliga myndigheter att utföra är enligt regeringens mening av allmänt intresse. Om uppgifterna inte vore av allmänt intresse skulle myndigheterna inte ha ålagts att utföra dem. På motsvarande sätt är de obligatoriska uppgifter som ålagts kommuner och landsting att utföra av allmänt intresse. Detta måste enligt regeringens mening gälla även i dataskyddsförordningens mening, eftersom det är upp till varje medlemsstat att fastställa de uppgifter som är av allmänt intresse.

Begreppet uppgifter av allmänt intresse omfattar dock inte bara sådant som utförs som en följd av ett offentligrättsligt och uttryckligt åliggande eller uppdrag. Till skillnad från vad som gäller enligt artikel 6.1 c i dataskyddsförordningen behöver den personuppgiftsansvarige inte vara skyldig att utföra uppgiften för att den rättsliga grunden i led e ska vara tillämplig.

Som en följd av det kommunala självstyret har kommuner och landsting en vidsträckt möjlighet att göra frivilliga åtaganden. Befogenheten är emellertid enligt kommunallagen (2017:725) begränsad till angelägenheter av just allmänt intresse. Kommuner och landsting får driva näringsverksamhet, men bara om den drivs utan vinstsyfte och syftar till att tillhandahålla allmännyttiga anläggningar eller tjänster åt medlemmarna. Som exempel på sådana uppgifter av allmänt intresse som kommunerna utför på frivillig grund kan nämnas tillhandahållande av bostäder och fritids- och idrottsanläggningar, åtgärder för att främja ortens näringsliv och annan kulturell verksamhet än bibliotek (som i stället är en obligatorisk uppgift).

Vissa myndigheter, t.ex. Lantmäteriet, har av riksdagen eller regeringen getts befogenhet att bedriva viss uppdragsverksamhet. Även

denna typ av verksamhet måste enligt regeringens mening anses vara motiverad av ett allmänt intresse.

Den verksamhet som en statlig eller kommunal myndighet bedriver, inom ramen för sin befogenhet, är således av allmänt intresse. Det är därmed den rättsliga grunden i artikel 6.1 e i dataskyddsförordningen som vanligen bör tillämpas av myndigheter, även utanför området för myndighetsutövning. Detta utesluter dock inte, som utredningen påpekar, att också andra rättsliga grunder samtidigt kan vara tillämpliga i vissa situationer.

Myndigheters verksamhet har stöd i rättsordningen

För att artikel 6.1 e i dataskyddsförordningen ska vara tillämplig räcker det inte att den verksamhet som myndigheterna bedriver är av allmänt intresse. Den måste också vara fastställd i enlighet med unionsrätten eller den nationella rätten. Som nämns ovan anges det i regeringsformen att den offentliga makten utövas under lagarna. Myndigheters verksamhet måste således ha stöd i någon av de källor som tillsammans bildar rättsordningen. Myndigheternas uppdrag och åligganden framgår av författningar, regeringsbeslut och kommunala reglementen, antagna i enlighet med regeringsformens bestämmelser om normgivningskompetens och kommunalt självstyre. De åtgärder som myndigheterna vidtar i syfte att utföra dessa uppdrag eller uppfylla dessa åligganden har därmed i sig en legal grund, som har offentliggjorts genom tydliga, precisa och förutsebara regler.

Statliga myndigheter får sina uppdrag och befogenheter av riksdag och regering – i myndighetsinstruktioner, regleringsbrev och andra regeringsbeslut. På motsvarande sätt följer de kommunala myndigheternas obligatoriska uppgifter av åligganden som fastställts i lag eller förordning. Även sådana frivilliga åtaganden som en kommun gör inom ramen för sin allmänna befogenhet ska framgå av gällande rätt, nämligen av det reglemente som fullmäktige utfärdar för den ansvariga nämnden.

Även privata aktörer kan utföra fastställda uppgifter av allmänt intresse

Vid tillämpningen av artikel 6.1 e spelar det ingen roll om den personuppgiftsansvarige är en offentlig eller en privat aktör. Om den uppgift som den personuppgiftsansvarige utför är av allmänt intresse och denna uppgift är fastställd i enlighet med unionsrätten eller den nationella rätten finns en rättslig grund för nödvändig behandling enligt artikel 6.1 e. Det saknar då betydelse om en privat aktör utför verksamheten på direkt uppdrag av en myndighet eller på eget initiativ.

Avmonopolisering och konkurrensutsättning av offentlig verksamhet i Sverige har inneburit att privaträttsliga organ numera utför en inte obetydlig del av de uppgifter som sannolikt skulle anses vara av allmänt intresse, även i begreppets mest snäva bemärkelse. Detta gäller inom den kommunala sektorn exempelvis avseende förskoleverksamhet och skola, hälso- och sjukvård samt stöd och service till funktionshindrade. Inom den traditionellt statliga sektorn kan nämnas rikstäckande infrastruktur, kommunikation och energiförsörjning. Ibland bedrivs verksamheten alltjämt under kommunal eller statlig styrning, i form av kommunala eller statliga bolag, men på andra områden förekommer också eller enbart

privata subjekt som är associationsrättsligt helt fristående från den offentliga sektorn.

I flera av dessa fall är verksamheten av kommersiell karaktär och bygger i viss utsträckning på avtal med den registrerade. I den mån behandling av personuppgifter är nödvändig kan den i sådana fall ske med stöd av artikel 6.1 b i dataskyddsförordningen, även om uppgiften inte skulle vara fastställd i lagstiftningen. När det gäller hälso- och sjukvårdsverksamhet, i både offentlig och privat regi, fastställs dock uppgiften i bl.a. hälso- och sjukvårdslagen (2017:30). På motsvarande sätt regleras uppgiften att tillhandahålla stöd och service till funktionshindrade av lagen (1993:387) om stöd och service till vissa funktionshindrade och uppgiften att tillhandahålla insatser inom socialtjänsten av socialtjänstlagen (2001:453). Skolväsendets uppgifter fastställs i skollagen (2010:800), som gäller för både offentliga och enskilda anordnare av utbildning.

De uppgifter av allmänt intresse som utförs i syfte att utföra ett uttryckligt uppdrag eller till följd av ett åliggande måste anses vara av denna karaktär oavsett om de faktiskt utförs i myndighetens egen regi eller om de genom utkontraktering eller entreprenad utförs av någon annan. När en juridisk eller fysisk person, på uppdrag av en kommunal eller statlig myndighet, utför en förvaltningsuppgift som åligger kommunen eller myndigheten, bör alltså även den privata utföraren, entreprenören eller det kommunala bolaget anses utföra en uppgift av allmänt intresse. Ett privaträttsligt organ som fullgör ett uppdrag från en myndighet avseende en sådan uppgift som är fastställd i författning, regeringsbeslut eller kommunalt beslut i fullmäktige kan därför vidta nödvändiga behandlingsåtgärder på samma rättsliga grund som om myndigheten själv utfört uppgiften, dvs. med stöd av artikel 6.1 e i dataskyddsförordningen. Det bör noteras att en uppdragstagare som är personuppgiftsbiträde åt myndigheten i stället behandlar personuppgifter med stöd av artikel 28 i dataskyddsförordningen.

När det är tveksamt om den verksamhet som en privaträttslig aktör, t.ex. ett statligt eller kommunalt bolag, bedriver är av allmänt intresse i unionsrättslig mening är det i stället ofta möjligt att grunda nödvändig behandling av personuppgifter på en intresseavvägning i enlighet med artikel 6.1 f i dataskyddsförordningen eller att inhämta den registrerades samtycke. Detsamma gäller om verksamheten visserligen är av allmänt intresse, men uppgiften inte är fastställd i enlighet med vare sig unionsrätten eller den nationella rätten.

Privata organ som omfattas av offentlighetsprincipen

Enligt artikel 86 i dataskyddsförordningen får personuppgifter i allmänna handlingar som förvaras av en myndighet eller ett offentligt organ eller ett privat organ för utförande av en uppgift av allmänt intresse lämnas ut av myndigheten eller organet i enlighet med den nationella rätt som myndigheten eller det offentliga organet omfattas av. Bestämmelsen möjliggör en tillämpning av tryckfrihetsförordningens bestämmelser om allmänhetens tillgång till allmänna handlingar när det gäller handlingar som innehåller personuppgifter. Detta innebär att den svenska grundlagsfästa handlingsoffentligheten är förenlig med dataskyddsförordningen.

Detta gäller enligt artikel 86 inte bara hos myndigheter och offentliga organ, utan även hos sådana privaträttsliga organ som utför uppgifter av allmänt intresse.

Offentlighetsprincipen gäller hos myndigheter, men inte hos alla privata organ som utför uppgifter av allmänt intresse. Tryckfrihetsförordningens bestämmelser om rätt att ta del av allmänna handlingar hos myndigheter ska dock enligt 2 kap. 3 § OSL i tillämpliga delar gälla också handlingar hos aktiebolag, handelsbolag, ekonomiska föreningar och stiftelser där kommuner eller landsting utövar ett rättsligt bestämmande inflytande. Enligt 2 kap. 4 § OSL ska rätten att ta del av allmänna handlingar hos myndigheter i tillämpliga delar också gälla handlingar hos de organ som anges i bilagan till offentlighets- och sekretesslagen, om handlingarna hör till den verksamhet som nämns där. Vissa av de organ som anges i den bilagan står under statlig styrning, medan andra är associationsrättsligt fristående från staten.

Gemensamt för de privata organ som enligt offentlighets- och sekretesslagen omfattas av offentlighetsprincipen är att de antingen anförtrotts förvaltningsuppgifter som rör myndighetsutövning eller att organets verksamhet helt eller delvis finansieras med allmänna medel. Detta innebär enligt regeringens mening att t.ex. Stiftelsen Svenska Filminstitutet och andra organ, vars handlingar omfattas av handlingsoffentlighet, i motsvarande utsträckning måste anses utföra uppgifter av allmänt intresse i den mening som avses i dataskyddsförordningen. Eftersom bestämmelsen i artikel 86 anger att även privata organ som utför uppgifter av allmänt intresse får lämna ut handlingar som innehåller personuppgifter, finns det således inte någon konflikt mellan offentlighetsprincipens tillämpning hos dessa organ och dataskyddsförordningen.

Svenska kyrkan undrar om det finns en konflikt mellan dataskyddsförordningen och det krav på att lämna ut handlingar som gäller i kyrkans verksamhet. Enligt 11 § lagen om Svenska kyrkan ska var och en ha rätt att ta del av Svenska kyrkans handlingar. Denna rätt får begränsas bara om det är särskilt motiverat med hänsyn till vissa särskilt angivna intressen. Den lagstadgade handlingsoffentlighet som gäller för dessa handlingar liknar således den som gäller i fråga om myndigheternas handlingar enligt tryckfrihetsförordningen. Enligt regeringens bedömning bör Svenska kyrkans handlingar därför betraktas som allmänna i den mening som avses i artikel 86 i dataskyddsförordningen. Dataskyddsförordningen ger således stöd för att Svenska kyrkan lämnar ut handlingar i enlighet med lagen om Svenska kyrkan.

Syftet med behandlingen ska vara nödvändigt

För att behandling av personuppgifter ska vara tillåten enligt artikel 6.1 e i dataskyddsförordningen krävs att ändamålet med behandlingen är nödvändigt för att utföra uppgiften. Detta ska enligt regeringens bedömning inte tolkas som att uppgiften av allmänt intresse måste vara avgränsad så att den bara kan utföras på ett sätt. Den metod som den personuppgiftsansvarige väljer för att utföra sin uppgift måste dock – som all offentlig förvaltning – vara ändamålsenlig, effektiv och proportionerlig och får därmed inte medföra ett onödigt intrång i enskildas privatliv. Ju mer detaljerat en viss uppgift har reglerats, desto mindre utrymme torde

det finnas för den personuppgiftsansvarige att välja olika tillvägagångssätt. Detta medför i sin tur en större förutsebarhet i fråga om vilken personuppgiftsbehandling som kan aktualiseras. Om ett uppdrag i stället har reglerats på en mer övergripande och resultatinriktad nivå kan det sannolikt utföras på många olika sätt, vilka i förhållande till varandra kan vara mer eller mindre nödvändiga i dataskyddsförordningens mening. Kravet på att ändamålet ska vara nödvändigt för att utföra en uppgift av allmänt intresse innebär alltså i sig en spärr mot helt onödig behandling av personuppgifter eller sådan behandling som utgör ett oproportionerligt intrång i privatlivet som inte kunnat förutses.

Alla myndigheter, såväl statliga som kommunala, vidtar en rad administrativa åtgärder som krävs för att myndigheten ska fungera. Som exempel kan nämnas myndigheternas interna säkerhetsarbete och information, personalvård samt, som bl.a. *Åklagarmyndigheten* påpekar, olika former av uppföljning och utvärdering av den egna verksamheten. Krav på myndigheterna att vidta sådana administrativa åtgärder kan framgå direkt eller indirekt av författning eller beslut. När det gäller myndigheternas säkerhetsarbete finns det t.ex. bestämmelser i förordningen om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap. I fråga om personalvård finns det bestämmelser i bl.a. arbetsmiljölagen (1977:1160). Allmänna krav på myndigheterna att följa upp och utvärdera den egna verksamheten följer av bestämmelserna i myndighetsförordningen (2007:515). Det förekommer dock även att myndigheterna, för att fungera, behöver vidta administrativa åtgärder som varken direkt eller indirekt kan sägas följa av författning eller beslut.

I skäl 27 till den rättsakt som gäller för EU-institutionernas personuppgiftsbehandling, förordning 45/2001, anges att behandling av personuppgifter för utförandet av de uppgifter av allmänt intresse som gemenskapsinstitutionerna och gemenskapsorganen utför inbegriper sådan behandling av personuppgifter som är nödvändig för förvaltningen av dessa institutioner och organ för att de ska fungera. En motsvarande skrivning finns i skäl 17 i kommissionens förslag till ny förordning på området (COM(2017) 8 final).

Någon motsvarighet till skäl 27 i förordning 45/2001 finns inte i dataskyddsförordningen. Bestämmelsen i artikel 6.3 andra stycket, om att syftet med behandlingen ska vara nödvändigt för att utföra uppgiften, fyller dock samma funktion. Den specifika behandlingen måste vara nödvändig för ett ändamål som i sin tur är nödvändigt för att myndigheten ska kunna utföra sitt uppdrag. Om myndigheten inte fungerar kan den inte utföra sina fastställda uppgifter. Behandling av personuppgifter som utförs som ett led i sådana administrativa åtgärder som är nödvändiga för myndighetens förvaltning och funktion är därmed enligt regeringens uppfattning rättsligt grundad i dataskyddsförordningens mening. Det krävs alltså inte att de administrativa åtgärderna är fastställda i enlighet med svensk rätt, så som *Datainspektionen* är inne på. Däremot måste de administrativa åtgärderna vara nödvändiga för att myndigheten ska kunna utföra sina uppgifter. Dessa uppgifter måste vara fastställda i enlighet med gällande rätt, vilket de som framgår ovan redan är.

Behov av förtydligande i nationell rätt

För att behandling av personuppgifter ska vara laglig enligt artikel 6.1 e i dataskyddsförordningen måste den uppgift som den personuppgiftsansvarige utför dels vara av allmänt intresse (eller utgöra ett led i myndighetsutövning), dels vara fastställd i enlighet med unionsrätten eller den nationella rätten. Vidare måste behandlingen vara nödvändig för ett ändamål som är nödvändigt för att utföra uppgiften. Detta framgår av direkt tillämpliga bestämmelser i dataskyddsförordningen. Det behövs därmed inte någon ytterligare nationell reglering, på generell nivå, för att sådan behandling av personuppgifter som är nödvändig för att utföra uppgifter av allmänt intresse ska kunna ske med stöd av den rättsliga grunden i artikel 6.1 e i förordningen. Detta gäller oavsett om den personuppgiftsansvarige är en offentlig eller en privat aktör.

Regeringen anser dock, i likhet med utredningen, att det finns anledning att ta in en bestämmelse i dataskyddslagen som tydliggör hur en uppgift av allmänt intresse ska fastställas för att kunna utgöra grund för behandling av personuppgifter. Uppgiften ska följa av lag eller annan författning eller av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning. En sådan upplysningsbestämmelse bidrar till förståelsen av dataskyddsregleringen och kan mot bakgrund av skäl 8 i förordningen inte anses vara en otillåten implementeringsåtgärd. Bestämmelsen bör utformas i linje med den formulering som används i artikel 6.1 e i dataskyddsförordningen. Regeringen föreslår därför en mindre justering av författningstexten jämfört med utredningens förslag.

Datainspektionen anser att det i bestämmelsen ska anges att kraven i artikel 6.3 andra stycket i dataskyddsförordningen måste följas. Som regeringen konstaterar i avsnitt 8.3 finns det dock inte skäl att införa ett sådant tillägg.

8.5 Behandling som ett led i myndighetsutövning

Regeringens förslag: Personuppgifter får behandlas om behandlingen är nödvändig som ett led i myndighetsutövning som den personuppgiftsansvarige utövar enligt lag eller annan författning.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Nästan alla remissinstanser tillstyrker förslaget eller har inga synpunkter på det. *Datainspektionen* anser att det i bestämmelsen ska anges att kraven i artikel 6.3 andra stycket måste följas. *Migrationsverket* och *Lunds universitet* anser att begreppet myndighetsutövning inte bör användas. Lunds universitet menar att det är svårt att tänka sig någon myndighetsutövning som inte utförs i allmänt intresse och att det därför riskerar att leda till oklarheter att särskilt nämna myndighetsutövning. *Dataskydd.net* anser att bestämmelsen är onödig.

Skälen för regeringens förslag: Enligt artikel 6.1 e i dataskyddsförordningen får personuppgifter behandlas bl.a. om behandlingen är nödvändig som ett led i den personuppgiftsansvariges myndighetsutövning. Begreppet myndighetsutövning förekommer även i dataskyddsdirektivet (artikel 7 e) och i personuppgiftslagen (10 § e) och har

en EU-gemensam innebörd. Utgångspunkten i svensk rätt är att det som i Sverige brukar anses som myndighetsutövning faller under begreppet (SOU 1997:39 s. 362). Detta bör gälla även fortsättningsvis.

Myndighetsutövning mot enskilda karaktäriseras av beslut eller andra ensidiga åtgärder som ytterst är uttryck för samhällets maktbefogenheter i förhållande till medborgarna. Myndighetsutövning kan också ske i förhållandet mellan myndigheter, t.ex. när en myndighet har tillsyn över en annan myndighets verksamhet. Utanför begreppet myndighetsutövning faller däremot råd, upplysningar och andra inte bindande uttalanden samt sådan faktisk verksamhet som inte innebär tvång. Av naturliga skäl är det i första hand statliga och kommunala myndigheter som ägnar sig åt myndighetsutövning. Även juridiska och fysiska personer kan dock med stöd av lag anförtros förvaltningsuppgifter som innefattar myndighetsutövning (12 kap. 4 § RF).

Enligt artikel 6.3 andra stycket första meningen i dataskyddsförordningen ska syftet med behandlingen, i fråga om behandling enligt punkt 1 e, vara nödvändigt som ett led i den personuppgiftsansvariges myndighetsutövning. Ändamålet med behandlingen behöver således inte, till skillnad från behandling som grundas på en rättslig förpliktelse, framgå av det sammanhang där befogenheten att utöva myndighet fastställs.

Kravet att ändamålet med behandlingen av personuppgifter måste vara nödvändigt för att utöva myndighetsutövningen ger uttryck för det samband som måste finnas mellan behandlingen och myndighetsutövningen. Detta samband framgår även av kravet i artikel 5.1 b på att de särskilda ändamålen ska vara berättigade.

Myndighetsutövning som medför skyldigheter för den enskilde eller i övrigt avser ingrepp i den enskildes personliga eller ekonomiska förhållanden måste enligt regeringsformen ha sin grund i lag eller i föreskrifter som meddelats med stöd av lag. Att meddela föreskrifter om åtgärder som är gynnande för den enskilde ryms däremot inom regeringens restkompetens. Myndighetsutövning kan även vara fastställd i enlighet med unionsrätten. Befogenhet att utöva myndighet fastställs i svensk rätt ofta direkt i den författning som reglerar en viss rättighet, skyldighet, åtgärd eller verksamhet. Befogenheten kan även framgå genom att en myndighet i lag eller förordning har pekats ut som behörig myndighet enligt en viss unionsrättsakt. Myndighetsutövning kan dock aldrig utövas utan stöd i gällande rätt.

Befogenhet att utöva myndighet i Sverige är således alltid fastställd i en författning. Det krävs därför inte någon ny nationell reglering på generell nivå för att sådan behandling av personuppgifter som är nödvändig som ett led i den personuppgiftsansvariges myndighetsutövning ska kunna ske med stöd av den rättsliga grunden i artikel 6.1 e i förordningen. Det bör noteras att denna rättsliga grund för behandling av personuppgifter kan tillämpas av alla personuppgiftsansvariga som tilldelats myndighetsutövande befogenheter.

Regeringen anser dock, i likhet med utredningen, att det finns anledning att ta in en bestämmelse i dataskyddslagen som tydliggör att myndighetsutövning utgör en rättslig grund för behandling av personuppgifter om myndighetsutövningen sker enligt lag eller annan författning. Detta är enligt skäl 8 till dataskyddsförordningen förenligt med unionsrätten, även om åtgärden kan sägas utgöra ett införlivande av en

direkt tillämplig förordningsbestämmelse. Eftersom begreppet myndighetsutövning används i dataskyddsförordningen anser regeringen till skillnad från *Migrationsverket* och *Lunds universitet* att det bör användas även i dataskyddslagen, trots att det inte förekommer i den nya förvaltningslagen och trots att det i princip inryms i begreppet uppgift av allmänt intresse.

Som regeringen konstaterar i avsnitt 8.3 finns det inte skäl att som *Datainspektionen* efterfrågar ange i bestämmelsen att kraven i artikel 6.3 andra stycket i dataskyddsförordningen måste följas.

8.6 Inledande upplysningsbestämmelse?

Regeringens bedömning: Det behövs inte någon bestämmelse som upplyser om att EU:s dataskyddsförordning anger att personuppgifter får behandlas endast om minst ett av de villkor som anges i artikel 6.1 i förordningen är uppfyllt.

Utredningens bedömning överensstämmer inte med regeringens. Utredningen föreslår en upplysningsbestämmelse.

Remissinstanserna: *Hovrätten för Västra Sverige*, *Kungliga tekniska högskolan* och *Swedish Direct Marketing Association* ifrågasätter behovet av en upplysningsbestämmelse. *Bolagsverket* anser att det bör införas en motsvarande hänvisning till artikel 5 i dataskyddsförordningen.

Skälen för regeringens bedömning: Dataskyddsförordningen är direkt tillämplig. I likhet med bl.a. *Hovrätten för Västra Sverige* och *Kungliga tekniska högskolan* anser regeringen att behovet av den upplysningsbestämmelse som utredningen föreslår angående rättslig grund kan ifrågasättas. Dataskyddslagen utgör endast ett komplement till förordningen och kan inte tillämpas självständigt. Som *Bolagsverkets* synpunkt indikerar är behovet av en upplysningsbestämmelse i fråga om artikel 6 inte större än det är avseende andra bestämmelser i dataskyddsförordningen, t.ex. artikel 5. Mot denna bakgrund anser regeringen att den upplysningsbestämmelse som utredningen föreslår riskerar att vara förvirrande i stället för vägledande. En sådan bestämmelse bör därför inte införas.

9 Barns samtycke som rättslig grund

Regeringens förslag: Vid erbjudande av informationssamhällets tjänster direkt till ett barn som bor i Sverige ska behandling av personuppgifter vara tillåten med stöd av barnets samtycke, om barnet är minst 13 år. Om barnet är under 13 år, ska sådan behandling vara tillåten endast om samtycke ges eller godkänns av den person som har föräldraansvar för barnet.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Majoriteten av remissinstanserna tillstyrker eller har inga invändningar mot utredningens förslag. Av de remissinstanser som särskilt yttrar sig i denna fråga anser t.ex. *Hovrätten för Västra Sverige*, *Kommerskollegium*, *Socialstyrelsen*, *Centrala studiestödsnämnden*, *Myndigheten för press, radio och TV*, *Falköpings kommun*, *Malmö kommun*, *Barnens Rätt i Samhället*, *Företagarna*, *Surfa Lugnt*, *Sveriges Radio AB*, *Sveriges Television AB*, *Swedish Direct Marketing Association*, *Dataspelsbranschen* och *Sveriges elevkårer* att en 13-årsgräns är att föredra. Flera av dessa remissinstanser, såsom Centrala studiestödsnämnden, Barnens Rätt i Samhället och Surfa Lugnt, framhåller att övervägande skäl talar för att åldersgränsen ska sättas lågt med hänsyn till det stora genomslag och betydelse som informationssamhällets tjänster har fått i unga personers liv, bl.a. som kommunikationskanal. Enligt Barnens Rätt i Samhället har barn som är 13 år och yngre insikt och förmåga att kunna fatta beslut med konsekvenser för den egna integriteten. *Svenskt Näringsliv* betonar att det finns en överhängande risk att den åldersgräns som införs i praktiken innebär en begränsning i användningen av olika nättjänster för barn och unga. Därutöver anser Svenskt Näringsliv att det är mest naturligt att utgå från en 13-årsgräns eftersom denna gräns gäller internationellt, t.ex. i USA. Myndigheten för press, radio och TV pekar på att barns rätt till yttrande- och informationsfrihet bör väga tungt och upplyser om att det i radio- och tv-lagen föreskrivs att reklam i tv-sändningar inte får syfta till att fånga uppmärksamheten hos barn under tolv år. *Forskningsrådet för hälsa, arbetsliv och välfärd* framhåller att förslaget är i linje med Sveriges syn om att värna barns rättigheter och integritet. Sveriges elevkårer tillägger att Sverige har en tradition av att skapa låga trösklar för att möjliggöra ungas engagemang och deltagande som samhällsmedborgare och att det därför är viktigt att fortsatt värna det demokratiska värdet av att ge barn och unga rätt till självbestämmande liksom yttrande- och informationsfrihet.

Surfa Lugnt ifrågasätter hur en bestämd åldersgräns i praktiken ska kunna följas. Kommerskollegium, som ifrågasätter om en åldersgräns överhuvudtaget kommer att leda till ett stärkt integritetsskydd, framför att en högre åldersgräns kan anses onödigt betungande för tjänsteleverantörer ur ett handelsperspektiv. Även Företagarna pekar på stora problem för tillhandahållare men också för användare av tjänsterna som kan komma att blockeras i sin användning av nättjänster med anledning av ålder. Malmö kommun lyfter bl.a. fram det förhöjda skydd som dataskyddsförordningen generellt ger vid behandling av barns personuppgifter. Att goda skyddsmekanismer kan uppnås genom dataskyddsförordningen och annan lagstiftning anser även Barnens Rätt i Samhället.

Om åldersgränsen bestäms till 13 år anser *länsstyrelserna i Kronobergs län* och *Stockholms län* att regleringen bör följas upp med utbildningsinsatser i hem och skola. Även Falköpings kommun lyfter fram att information om personuppgiftsbehandling bör ingå som en del i att öka elevers digitala kompetens. Sveriges elevkårer anser också att information och dialog om beteenden på internet är bättre än att utestänga barn från sociala nätverksforum. Surfa Lugnt instämmer i att en utökad och förbättrad dialog kring internet mellan barn och vuxna är viktig. Barnens Rätt i Samhället framhåller att det hade varit önskvärt med ett förslag om

att Datainspektionen ska kunna ta fram en sammanfattning av lagtexten på lättbegriplig svenska i syfte att spridas som information i skolor för att barn lättare ska tillgodogöra sig innehållet.

Några remissinstanser, såsom *Kammarrätten i Göteborg*, *Barnombudsmannen*, *Datainspektionen*, *Mörbylånga kommun*, *Jönköpings läns landsting* och *Sveriges läkarförbund*, anser, bl.a. med utgångspunkt i hur åldersgränsen för barns samtycke och möjlighet att agera i rättsliga och andra sammanhang är satt i Sverige, att det finns skäl att överväga en åldersgräns om 15 år. Datainspektionen betonar att den hittills tillämpade åldersgränsen för när barn normalt ska anses förstå innebörden och konsekvenserna av en viss behandling av personuppgifter och därmed kunna ge sitt samtycke till den är 15 år. *Skolinspektionen*, *Skolverket* och *Dorotea kommun* är av samma uppfattning. Skolinspektionen hänvisar också till sin granskning som visar att elevers interaktion på internet ofta sker utan insyn av vuxna vilket medför att kränkningar på internet kan vara svåra att upptäcka och utreda. Enligt Skolinspektionen skulle integritetsskyddet för unga öka markant med en åldersgräns om 15 år.

Ett antal remissinstanser, såsom *Riksdagens ombudsmän*, *Förvaltningsrätten i Linköping*, *Försäkringskassan*, *Pensionsmyndigheten*, *Östergötlands läns landsting*, *länsstyrelserna i Värmland, Skåne och Stockholms län*, *Specialpedagogiska skolmyndigheten*, *Lunds universitet*, *Grästorps kommun*, *Stiftelsen för internetinfrastruktur* och *Lärarnas riksförbund*, avstyrker eller är tveksamma till utredningens förslag och menar bl.a. att det underlag som utredningen presenterar inte är tillräckligt för att avvika från förordningens 16-årsgräns liksom att 13 år är en för lågt satt åldersgräns. *Folkhälsomyndigheten* understryker att utredningens förslag vilar på ett bristfälligt kunskapsunderlag där resonemanget till stora delar saknar ett barnperspektiv. Förvaltningsrätten i Linköping framför att barn utgör en utsatt grupp som måste ha ett särskilt skydd och att ett barn bör ha uppnått en sådan ålder att han eller hon förstår vad samtycket avser och konsekvenserna av det. Enligt Stiftelsen för internetinfrastruktur är det inte relevant vilka andra skyddsmekanismer som finns för att ”rätta till” det ogiltiga samtycket.

Några remissinstanser, t.ex. *Förvaltningsrätten i Jönköping*, *Uppsala universitet*, *Umeå universitet*, Länsstyrelsen i Kronobergs län, *Västerbottens läns landsting* och Östergötlands läns landsting efterfrågar en närmare analys av frågan om åldersgräns. Kammarrätten i Göteborg, *Polismyndigheten*, Datainspektionen, Försäkringskassan, Socialstyrelsen, *Karlskrona kommun* och *Sveriges Kommuner och Landsting* framhåller vikten av en harmonisering av åldersgränsen för barns samtycke till personuppgiftsbehandling. Av det skälet menar flera av dessa remissinstanser att det är tveksamt att avvika från förordningens 16-årsgräns. Företagarna menar dock att det saknas behov av att anpassa åldersgränsen efter andra länders val.

Kammarrätten i Göteborg föreslår att uttrycket den person som har föräldraansvar i den föreslagna paragrafen ändras till barnets vårdnadshavare. Länsstyrelsen i Kronobergs län betonar att det i förslaget bör förtydligas om ett samtycke krävs från båda vårdnadshavarna vid gemensam vårdnad.

Östergötlands läns landsting och *Sveriges advokatsamfund* anser att begreppet informationssamhällets tjänster behöver utredas vidare. *Statis-*

tiska centralbyrån väcker frågan om även tjänster på distans, som sker elektroniskt via en individuell begäran av en tjänstemottagare, men utan ersättning och som erbjuds av t.ex. en myndighet omfattas av begreppet informationssamhällets tjänster. När det gäller begreppet direkt till barn delar Kommerskollegium utredningens tolkning att begreppet bör ta sikte på sådana tjänster som kan antas användas av barn. Barnens Rätt i Samhället efterlyser ett förtydligande av formuleringen förebyggande och rådgivande tjänster som erbjuds direkt till barn som föreskrivs i skäl 38 i förordningen och konkreta exempel på hur krav på utformning av information och samtycke ur ett barnperspektiv kan uppfyllas. Surfa Lugnt föreslår att en myndighet eller organisation ska få i uppgift att utvärdera konsekvenserna av ett införande av en åldersgräns.

Skälen för regeringens förslag

Allmänt om regleringen i dataskyddsförordningen

För att en personuppgiftsbehandling ska vara laglig krävs att det finns en rättslig grund för behandlingen enligt artikel 6 i dataskyddsförordningen. Samtycke från den registrerade utgör enligt artikel 6.1 a en sådan rättslig grund. I artikel 8.1 i dataskyddsförordningen anges att vid erbjudande av informationssamhällets tjänster direkt till ett barn, ska behandling av personuppgifter få ske med stöd av den registrerades samtycke om barnet är minst 16 år. Om barnet är under 16 år ska sådan behandling vara tillåten endast om och i den mån samtycket ges eller godkänns av den person som har föräldraansvar för barnet. Medlemsstaterna får föreskriva en lägre ålder i sin nationella rätt, under förutsättning att denna ålder inte är lägre än 13 år. I skäl 38 uttalas att barns personuppgifter förtjänar ett särskilt skydd, eftersom barn kan vara mindre medvetna om risker, skyddsåtgärder och rättigheter. Det särskilda skyddet bör i synnerhet gälla användningen av barns personuppgifter i marknadsföringssyfte, för att skapa personlighets- eller användarprofiler samt för insamling av uppgifter när tjänster som erbjuds direkt till barn utnyttjas. Samtycke från den person som har föräldraansvar över ett barn bör enligt skältexten inte krävas för förebyggande eller rådgivande tjänster som erbjuds direkt till barn. I likhet med *Barnens Rätt i Samhället* anser regeringen att det ligger närmast till hands att tolka förebyggande eller rådgivande tjänster som erbjuds direkt till barn som tjänster som enbart innefattar insatser direkt riktade mot utsatta barn och att det är önskvärt att uttrycket inte får en alltför bred tolkning. Det kan dock konstateras att den aktuella begränsningen av kravet på samtycke från den person som har föräldraansvaret inte återfinns i artikeltexten och att den närmare innebörden är oklar.

Det är enligt dataskyddsförordningen endast vid erbjudande av informationssamhällets tjänster till någon som är under 16 år som samtycket till behandlingen av personuppgifter behöver ges eller godkännas av den som har föräldraansvaret för barnet. När det gäller personuppgiftsbehandling som sker i andra sammanhang får en bedömning, liksom tidigare, göras i varje enskilt fall av den registrerades förmåga att förstå innebörden av ett lämnat samtycke.

Begreppet informationssamhällets tjänster

Informationssamhällets tjänster är ett EU-rättsligt begrepp och definieras i artikel 4.25 i dataskyddsförordningen som alla tjänster enligt definitionen i artikel 1.1 b i Europaparlamentets och rådets direktiv (EU) 2015/1535 av den 9 september 2015 om ett informationsförfarande beträffande tekniska föreskrifter och beträffande föreskrifter för informationssamhällets tjänster (direktiv 2015/1535). I sistnämnda artikel anges att informationssamhällets tjänster är tjänster som vanligtvis utförs mot ersättning, på distans, på elektronisk väg och på individuell begäran av en tjänstemottagare. I denna artikel anges vidare att med på distans avses att tjänsten tillhandahålls utan att parterna är närvarande samtidigt. Med på elektronisk väg avses att tjänsten sänds vid utgångspunkten och tas emot vid slutpunkten med hjälp av utrustning för elektronisk behandling och lagring av uppgifter och i sin helhet sänds, befordras och tas emot genom tråd, radio, optiska medel eller andra elektromagnetiska medel. Med på individuell begäran av en tjänstemottagare avses att tjänsten tillhandahålls genom överföring av uppgifter på individuell begäran.

Begreppet används även i bl.a. Europaparlamentets och rådets direktiv 2000/31/EG av den 8 juni 2000 om vissa rättsliga aspekter på informationssamhällets tjänster, särskilt elektronisk handel, på den inre marknaden (e-handelsdirektivet). Vid tolkningen av begreppet har EU-domstolen konstaterat att det inte krävs att tjänsten betalas av den som åtnjuter tjänsten för att den ska omfattas av definitionen. Tjänsten kan t.ex. finansieras genom inkomster via reklam som visas på en webbplats (dom Papasavvas, C-291/13, EU:C:2014:2209, punkterna 28–30). Redan definitionen av begreppet i direktiv 2015/1535 indikerar att ersättning inte nödvändigtvis måste utgå vid utförandet av tjänsten och att det, som *Statistiska centralbyrån* lyfter fram, inte finns något direkt hinder mot att en sådan tjänst erbjuds av t.ex. en myndighet. När e-handelsdirektivet genomfördes i svensk rätt uttalade dock regeringen att med informationssamhällets tjänster avses – förenklat uttryckt – varje aktivitet som sker online, med någon ekonomisk innebörd. Regeringen menade att begreppet omfattar en mängd olika tjänster, däribland informationstjänster och söktjänster (prop. 2001/02:150 s. 1 och 19). Begreppet informationssamhällets tjänster kan enligt sin definition också innefatta bl.a. olika sociala medier, t.ex. bloggar, internetforum, webbplatser för videoklipp, chattprogram och sociala nätverk. Även onlinespel och olika applikationer (appar) för smarta enheter kan omfattas av definitionen. Eftersom det är fråga om ett EU-rättsligt begrepp är det vanskligt att, som *Östergötlands läns landsting* och *Sveriges advokatsamfund* efterlyser, ge ytterligare vägledning om begreppets innebörd.

Vissa av informationssamhällets tjänster kan tillhandahållas och användas utan att någon behandling av personuppgifter sker. I praktiken är det emellertid mycket vanligt att användaren måste dela med sig av vissa personuppgifter för att kunna utnyttja tjänsten. Vilka personuppgifter som samlas in, hur de används av tjänstetillhandahållaren själv och hur dessa uppgifter delas med andra varierar från tjänst till tjänst. De uppgifter som samlas in kan vara uppgifter som den enskilde måste uppge för att få använda en tjänst, såsom ett namn, användarnamn, födelsedatum, kön, adress, e-postadress och mobiltelefonnummer. Det

kan även vara uppgifter om kreditkorts- och betalningsinformation. Ofta behandlas också personuppgifter vid användningen av en tjänst. Det kan röra sig om bl.a. geografiska lokaliseringsuppgifter eller uppgifter om vem användaren interagerar med. Även webbläsarhistorik kan skapas och bli föremål för senare behandling. Uppgifter kan också synkroniseras med andra användares uppgifter, exempelvis uppgifter från adressboken på en telefon. Uppgifterna kan användas i olika syften, t.ex. för direktmarknadsföring.

Uttrycket direkt till barn

Det framgår inte av dataskyddsförordningen vad som avses med uttrycket att en tjänst ska erbjudas direkt till barn. Det skulle kunna tolkas på flera olika sätt. En möjlig tolkning är att det endast omfattar tjänster som uttryckligen riktar sig till barn. Det skulle också kunna vara användarens faktiska ålder som avgör om tjänsten omfattas av uttrycket. Regeringen anser, i likhet med utredningen, att mycket talar för att det avgörande bör vara om tjänsten kan antas användas av barn. Bedömningen blir då inte beroende av hur tjänsteleverantören presenterar sin tjänst utåt. Både tjänster som direkt marknadsförs mot barn och tjänster som i och för sig inte marknadsförs som särskilt anpassade för barn, men som på grund av sin utformning eller sitt innehåll och funktion är av det slaget att de typiskt sett kan antas användas av barn, omfattas vid en sådan tolkning av bestämmelsen. Uttrycket direkt till barn är emellertid EU-rättsligt och det är EU-domstolen som ytterst kan ge vägledning för tolkningen.

Uttrycket den person som har föräldraansvar för barnet

Som framgår ovan förekommer uttrycket den person som har föräldraansvar i artikel 8.1 i dataskyddsförordningen. Vad som avses med uttrycket framgår dock inte av förordningen och *Länsstyrelsen i Kronobergs län* efterlyser därför närmare vägledning om hur det bör tolkas.

Begreppet föräldraansvar förekommer också i artikel 2.7 i förordningen (EG) nr 2201/2003 om domstols behörighet och om erkännande och verkställighet av domar i äktenskapsmål och mål om föräldraansvar samt om upphävande av förordning (EG) nr 1347/2000 (Bryssel II-förordningen). I den förordningen definieras föräldraansvar som alla rättigheter och skyldigheter som en fysisk eller juridisk person har tillerkänts genom en dom, på grund av lag eller genom en överenskommelse med rättslig verkan, med avseende på ett barn eller dess egendom. Det anges vidare att föräldraansvar omfattar bl.a. vårdnad och umgänge. På motsvarande sätt definieras föräldraansvar i artikel 1.2 i den i Haag den 19 oktober 1996 dagtecknade konventionen om behörighet, tillämplig lag, erkännande, verkställighet och samarbete i frågor om föräldraansvar och åtgärder till skydd för barn (1996 års Haagkonvention). I Sverige finns regler om barn och deras ställföreträdare i föräldrabalken. Den som har vårdnaden om ett barn har ansvar för barnets personliga förhållanden. Därmed har vårdnadshavaren rätt och skyldighet att bestämma i olika frågor som rör barnet.

Enligt regeringens bedömning bör med uttrycket den person som har föräldraansvar för barnet i dataskyddsförordningen i första hand avses ett barns vårdnadshavare eller någon annan med uppdrag att vara i vårdnadshavarens ställe, t.ex. god man för ensamkommande barn. Om uttrycket skulle ges motsvarande innebörd som i Bryssel II-förordningen kan dock även andra omfattas, exempelvis föräldrar med umgängesrätt. Eftersom uttrycket är EU-rättsligt är det ytterst EU-domstolen som avgör dess innebörd. Det är mot denna bakgrund inte möjligt att, som *Kammarrätten i Göteborg* föreslår, ersätta uttrycket med vårdnadshavare.

Det finns ingen reglerad åldersgräns i dag

Det finns i dag ingen uttrycklig reglering vare sig i dataskyddsdirektivet eller i personuppgiftslagen om barns samtycke till personuppgiftsbehandling. En bedömning av om den underåriges samtycke ska anses utgöra rättslig grund för personuppgiftsbehandling har därför fått göras från fall till fall.

Datainspektionen har uttalat att det krävs att den som ger samtycket kan förstå innebörden av det. En person som inte själv kan tillgodogöra sig informationen om vad ett samtycke till personuppgiftsbehandling innebär kan inte ge ett rättsligt bindande samtycke. Datainspektionen har vidare ansett att barn under 15 år i allmänhet inte kan anses ha nått en sådan mognad att de kan förstå innebörden av att samtycka till personuppgiftsbehandling. Samtidigt har Datainspektionen i ett samrådsyttrande som rörde användande av personnummer som spärr för deltagande på en chattsajt framhållit att föräldrarnas samtycke till barns registrering av sina personuppgifter måste inhämtas i vart fall när det gäller barn som inte har fyllt 13 år (SOU 2017:39 s. 137 och 138). Detta visar att det inte är helt tydligt vad som i dag gäller i frågan om åldersgräns för barns samtycke till personuppgiftsbehandling.

I Sverige får en omyndig person, dvs. en person som är under 18 år, som huvudregel inte själv råda över sin egendom eller åta sig förbindelser. Det finns dock ett antal undantag från denna huvudregel. I vissa sammanhang får barnet självt ingå rättshandlingar och föra sin talan. Dessutom ska ibland barnets samtycke ges avgörande betydelse. I flera författningar, t.ex. 21 kap. 5 § föräldrabalken och 4 kap. 3 § patientlagen (2014:821), föreskrivs även att barnets vilja ska tillmätas betydelse med ökad ålder och mognad. När det gäller barnets möjligheter att ingå avtal och sköta andra angelägenheter av ekonomisk natur gäller i vissa fall en åldersgräns om 16 år. I några enstaka fall har åldersgränsen bestämts till 12 år. Denna åldersgräns gäller t.ex. vid samtycke till adoption och när reklam i tv-sändningar får syfta till att fånga uppmärksamheten hos barn. I andra sammanhang har åldersgränsen för barns samtycke och möjlighet att själva agera ofta satts vid 15 år. Barn som har fyllt 15 år har t.ex. rätt att själva föra sin talan i mål och ärenden enligt lagen (1990:52) med särskilda bestämmelser om vård av unga. Vidare kan en person som har fyllt 15 år dömas till påföljd för brott som han eller hon begått. Dessutom är sexuellt umgänge med barn kriminaliserat endast såvitt gäller barn under 15 år.

I svensk lag är det således ovanligt att det stipuleras en lägre åldersgräns än 15 år. Detta talar enligt regeringens mening för att

åldersgränsen i Sverige för att kunna lämna ett giltigt samtycke inte bör sättas lägre än 15 år. Samtidigt talar bl.a. avsaknaden av en lagstadgad åldersgräns – och det förhållandet, som *Svenskt Näringsliv* framhåller, att de flesta bolag som riktar sig till unga med digitala varor och tjänster utgår från den 13-årsgräns som föreskrivs i amerikansk rätt – för att åldersgränsen bör vara så låg som förordningen medger. Även barns yttrande- och informationsfrihet samt självbestämmelserätt talar för det. Se vidare nedan.

Olika åldersgränser gäller i olika länder

Ett antal remissinstanser, t.ex. *Datainspektionen*, pekar på den harmoniseringstanke som genomsyrar dataskyddsreformen och framhåller vikten av en harmonisering av åldersgränsen. I pågående lagstiftningsarbeten i andra länder behandlas bl.a. frågan om en åldersgräns för barns samtycke till personuppgiftsbehandling. Det faktum att den aktuella regleringen i dataskyddsförordningen ger nationell flexibilitet visar dock att harmonisering inte har ansetts avgörande i denna fråga. Till bilden hör också, som exempelvis *Svenskt Näringsliv* poängterar, att en 13-årsgräns gäller i några andra länder, t.ex. i USA. Detta talar för att Sverige bör välja en åldersgräns om 13 år.

Barn har yttrande- och informationsfrihet samt självbestämmanderätt

Som flera remissinstanser, t.ex. *Myndigheten för press, radio och TV* och *Sveriges elevkårer*, framhåller måste stor vikt fästas vid de fri- och rättigheter som barn åtnjuter. I FN:s konvention om barnets rättigheter, den s.k. barnkonventionen, anges bl.a. att konventionsstaterna ska tillförsäkra det barn som är i stånd att bilda egna åsikter rätten att fritt uttrycka dessa i alla frågor som rör barnet, varvid barnets åsikter ska tillmätas betydelse i förhållande till barnets ålder och mognad. Barnkonventionen slår också fast att barnet har rätt till yttrandefrihet. Denna rätt innefattar frihet att oberoende av territoriella gränser söka, motta och sprida information och tankar av alla slag, i tal, skrift eller tryck, i konstnärlig form eller genom annat uttrycksmedel som barnet väljer.

Det finns anledning att understryka att föräldrar och andra vårdnadshavare har både en rätt och en skyldighet att ge barnet lämplig ledning och råd vid utövandet av barnets rättigheter. Vägledning ska ges på ett sätt som överensstämmer med barnets fortlöpande utveckling. Barnet ska alltså med stigande ålder få större möjlighet att själv styra över på vilket sätt det vill ta vara på sina rättigheter. Eftersom barn håller på att utvecklas fysiskt och psykiskt, måste dock utövandet av barnets rättigheter anpassas till dess utvecklingsnivå.

Dagens barn och unga använder internet bl.a. för att ta del av information, sprida åsikter liksom förmedla tankar och därigenom utöva de fri- och rättigheter som beskrivs ovan. Som flera remissinstanser konstaterar har tillgången till information via söktjänster och deltagandet i olika onlineaktiviteter stor social betydelse för barn och unga. Det är ett sätt att skapa och behålla kontakt med kamrater, delta i politiska och andra diskussionsforum, söka information till skolarbeten, spela spel, se på film och lyssna på musik. Studier visar att användningen av sociala nätverkssajter, såsom Facebook, Instagram och Kik, har ökat markant de senaste

åren (SOU 2016:41 s. 374–376). En hög åldersgräns för när ett barn själv kan ge giltigt samtycke till personuppgiftsbehandling kan i praktiken leda till att barn i mitten av sin tonårstid utestängs från möjligheten till social och kulturell samvaro inom ramen för det som avses med informationssamhällets tjänster, om dess vårdnadshavare inte samtycker till den personuppgiftsbehandling som krävs för att barnet ska kunna använda tjänsten. Detta kan i sin tur leda till en inskränkning i barnets rätt att fritt söka information och uttrycka sig i olika sammanhang. Det innebär också en begränsning av barnets självbestämmanderätt. Dessa oönskade effekter talar med styrka för att åldersgränsen bör bestämmas till den lägsta tillåtna, dvs. 13 år. Samtidigt måste de oönskade effekterna vägas emot de integritetsvinster som en högre åldersgräns skulle kunna ge.

Det finns tillräckliga skyddsmekanismer

Integritetsriskerna för barn som använder informationssamhällets tjänster är i första hand kopplade till att ett samtycke i de flesta fall innebär att en stor mängd uppgifter om barnet kan lagras och spridas i marknadsföringssyfte. Direktmarknadsföring är ofta ett grundläggande inslag i affärsmodellen för sociala nätverkstjänster och andra typer av informationssamhällets tjänster. Användarnas personuppgifter samlas in och sparas, bl.a. för att beteendebaserad reklam ska kunna riktas till användaren. Detta kan betraktas som en slags kartläggning av användarnas personliga förhållanden, i den mån de kommer till uttryck i deras aktiviteter online, t.ex. vid användning av en söktjänst eller ett socialt medium. En sådan kartläggning kan, särskilt om den pågår under lång tid, i sig medföra stora risker för intrång i den personliga integriteten.

Flera remissinstanser invänder mot utredningens förslag av den anledningen att ett barn vid 13 års ålder inte har uppnått en sådan mognad att det kan förstå innebörden och konsekvenserna av ett samtycke. Samtidigt menar *Barnens Rätt i Samhället* att barn som är 13 år och yngre har insikt och förmåga att kunna fatta beslut med konsekvenser för den egna integriteten. Att förstå i vilken utsträckning och för vilket syfte personuppgifter behandlas i samband med att en tjänst erbjuds och används kräver, som utredningen uttalar, en hög grad av insikt och mognad. Det kan vara komplex information att ta till sig och det kan vara svårt att förstå och värdera riskerna med personuppgiftsbehandlingen. Regleringen i dataskyddsförordningen innebär dock att det ställs höga krav på tjänstetillhandahållarna att utforma informationen om vad ett samtycke innebär, särskilt i förhållande till barn, för att samtycket ska ses som giltigt i förordningens mening.

För att förstå innebörden och konsekvenserna av ett samtycke menar regeringen, i likhet med bland andra *Falköpings kommun*, att en avgörande förutsättning är att barn och unga erhåller information som syftar till att öka deras digitala kompetens. I detta sammanhang kan nämnas att regeringen i mars 2017 beslutade om förtydliganden och förstärkningar i bl.a. läroplaner, kursplaner och ämnesplaner för grundskolan och gymnasieskolan i syfte att tydliggöra skolans uppdrag att stärka elevernas digitala kompetens (U2017/01134/S). Vidare beslutade regeringen i oktober 2017 om en nationell digitaliseringsstrategi där det övergripande målet för skolväsendet är att det svenska skolväsendet ska

vara ledande i att använda digitaliseringens möjligheter på bästa sätt för att uppnå en hög digital kompetens hos barn och elever och för att främja kunskapsutvecklingen och likvärdigheten (U2017/04119/S).

Liksom *Förvaltningsrätten i Linköping* anser regeringen att barn måste ha ett starkt skydd för den personliga integriteten. Det kan emellertid konstateras att redan de allmänna bestämmelserna om samtycke i dataskyddsförordningen ger ett starkt skydd. Av artikel 7.2 framgår att en begäran om samtycke ska läggas fram på ett sätt som klart och tydligt kan särskiljas från de andra frågorna i en begriplig och lätt tillgänglig form, med användning av ett klart och tydligt språk. Enligt artikel 7.3 ska den registrerade när som helst ha rätt att återkalla samtycket. Dataskyddsförordningen ger också ett särskilt starkt skydd för barn i vissa avseenden. I skäl 38 uttalas att barns personuppgifter förtjänar ett särskilt skydd, eftersom barn kan vara mindre medvetna om risker, skyddsåtgärder och rättigheter. Det särskilda skyddet bör, enligt samma skäl, i synnerhet gälla användningen av barns personuppgifter i marknadsföringssyfte, för att skapa personlighets- eller användarprofiler samt för insamling av uppgifter när tjänster som erbjuds direkt till barn utnyttjas. Av artikel 12.1 och skäl 58 följer att information och kommunikation som riktar sig till barn ska utformas på ett tydligt och enkelt språk som barnet lätt kan förstå. Det är i nuläget inte möjligt att, som *Barnens Rätt i Samhället* efterfrågar, ge närmare vägledning för hur samtycket och informationen till barn bör utformas. Enligt artikel 57.1 b i dataskyddsförordningen ska dock varje tillsynsmyndighet ansvara för att bl.a. öka allmänhetens medvetenhet om och förståelse för risker, regler, skyddsåtgärder och rättigheter i fråga om behandling. Särskild uppmärksamhet ska ägnas åt insatser som riktar sig till barn. Inom detta ansvar skulle sådana insatser som att ta fram sammanfattningar av lagtexten på lättbegriplig svenska, som Barnens Rätt i Samhället föreslår, kunna ingå.

Det finns vidare, som utredningen pekar på, även annan lagstiftning på t.ex. marknadsföringsområdet och branschpraxis som syftar till att hindra att barns personuppgifter används i marknadsföringssyfte. Enligt svensk rätt strider det även som huvudregel mot god marknadsföringssed att rikta direktreklam till barn under 16 år (se MD 1999:26 och MD 2012:14).

I likhet med utredningen bedömer regeringen att det finns tillräckliga skyddsmekanismer för att förhindra omfattande insamling och annan behandling av barns personuppgifter i marknadsföringssyfte och som minskar riskerna i samband med att barn lämnar samtycke till behandling av personuppgifter vid användningen av informationssamhällets tjänster.

Sammanfattande bedömning

Tillgången till information via söktjänster och deltagandet i olika onlineaktiviteter har stor social betydelse för barn och unga. Genom olika tjänster på internet kan barn och unga i dag ta del av information, bilda sin egen åsikt och förmedla sina tankar på ett enkelt sätt och därigenom utöva flera av de fri- och rättigheter som kommer till uttryck i barnkonventionen. En hög åldersgräns för när ett barn själv kan lämna ett giltigt samtycke till personuppgiftsbehandling kan leda till att barn utestängs från möjligheten att delta i och utnyttja sådana sociala medier

som innefattas i begreppet informationssamhällets tjänster. Enligt regeringens mening finns det tillräckliga skyddsmekanismer för att skydda barn både i dataskyddsregleringen och inom marknadsrätten. Regeringen bedömer därför att vikten av barns rätt till självbestämmande och yttrande- och informationsfrihet väger tyngre än det ökade integritetsskydd som en hög åldersgräns skulle kunna leda till. Till skillnad från t.ex. *Riksdagens ombudsmän* och *Förvaltningsrätten i Linköping* anser regeringen att det finns tillräckligt underlag för att komma fram till slutsatsen att barn som har fyllt 13 år själva ska kunna samtycka till personuppgiftsbehandling i samband med att informationssamhällets tjänster erbjuds direkt till barn. Det kan dock finnas anledning att, som *Surfa Lugnt* föreslår, vid behov återkomma till frågan och i framtiden utvärdera konsekvenserna av den reglerade åldersgränsen.

10 Känsliga personuppgifter

10.1 Förbudet och undantagen föreskrivs i dataskyddsförordningen

Regeringens förslag: Personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa och uppgifter om en fysisk persons sexualliv eller sexuella läggning ska i dataskyddslagen benämnas *känsliga personuppgifter*.

Regeringens bedömning: Behandling av känsliga personuppgifter får ske endast under de förutsättningar som anges i EU:s dataskyddsförordning. Undantagen från förbudet mot behandling är direkt tillämpliga.

Utredningens förslag och bedömning överensstämmer delvis med regeringens. Utredningen bedömer att vissa av undantagen i sig måste föreskrivas i nationell rätt, antingen i generell eller i sektorsspecifik reglering, för att vara tillämpliga. Vidare föreslår utredningen en upplysningsbestämmelse avseende behandling av känsliga personuppgifter.

Remissinstanserna: Det stora flertalet remissinstanser instämmer i utredningens bedömning eller kommenterar den inte. *Polismyndigheten* anser att begreppet känsliga personuppgifter, som är väl inarbetat, inte bör utökas till att omfatta genetiska och biometriska uppgifter. *Vetenskapsrådet* och *Sveriges advokatsamfund* anser att begreppet särskilda kategorier av personuppgifter bör användas i stället för begreppet känsliga personuppgifter. *Förvaltningsrätten i Stockholm* efterfrågar förtydliganden avseende skillnaden mellan nödvändighetsrekvisitets innebörd i artiklarna 6 och 9 samt anser att upplysningsbestämmelsen har en något svår lagteknisk lösning. *Datainspektionen* anser att det är en brist att utredningen inte gjort någon analys av hur de föreslagna undantagsbestämmelserna för behandling av känsliga personuppgifter förhåller sig

till kravet på rättslig grund. *Pensionsmyndigheten* anser inte att det är självklart att det finns ett behov av att i dataskyddslagen eller i annan nationell lagstiftning ta in bestämmelser om undantag från förbudet att behandla känsliga personuppgifter. *Dataskydd.net* anser att upplysningsbestämmelsen ska tas bort och att utredningen missar poängen med bestämmelserna i artikel 9.2 b, g, h, i och j.

Skälen för regeringens bedömning: Enligt dataskyddsförordningen måste all behandling av personuppgifter vila på en rättslig grund. En grundläggande förutsättning för behandling är således att någon av de rättsliga grunder som anges i artikel 6 är tillämpliga. Dessutom ska den personuppgiftsansvarige följa de principer för behandlingen som framgår av artikel 5. För vissa typer av personuppgifter måste därutöver särskilda krav vara uppfyllda för att behandling ska få ske.

Enligt artikel 9.1 i dataskyddsförordningen är det förbjudet att behandla uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening samt genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa och uppgifter om en fysisk persons sexualliv eller sexuella läggning. Bestämmelsen är direkt tillämplig och kräver inga åtgärder av medlemsstaterna.

Ett liknande förbud finns i artikel 6 i dataskyddskonventionen och i artikel 8.1 i dataskyddsdirektivet. Genetiska och biometriska uppgifter liksom uppgifter om sexuell läggning är dock nya kategorier som lagts till i dataskyddsförordningen.

I såväl direktivet som förordningen anges det i rubriken till bestämmelsen att den avser behandling av särskilda kategorier av personuppgifter. I förordningens skäl 10 och 51 omnämns dessa uppgifter i stället som känsliga respektive särskilt känsliga uppgifter. I personuppgiftslagen och andra svenska författningar används benämningen känsliga personuppgifter. Det begreppet är väl inarbetat, även på EU-nivå, och är språkligt enklare att använda och förstå, inte minst i författningstext. Regeringen anser därför, till skillnad från *Polismyndigheten* och *Sveriges advokatsamfund*, att begreppet känsliga personuppgifter bör användas i dataskyddslagen som samlingsbenämning för sådana uppgifter som tillhör de särskilda kategorier av personuppgifter som anges i artikel 9 i dataskyddsförordningen.

Förordningens förbud ska enligt artikel 9.2 inte tillämpas om någon av de situationer som beskrivs i punkterna a–j föreligger. Något utrymme för medlemsstaterna att föreskriva ytterligare undantag från förbudet lämnas inte. Däremot får medlemsstaterna behålla eller införa mer specifika bestämmelser i fråga om behandling som sker med stöd av artikel 6.1 c och e, även när det gäller känsliga personuppgifter (artikel 6.2 och skäl 10). Vissa av undantagen i artikel 9.2 innehåller också uttryckliga hänvisningar till och krav på innehållet i unionsrätten och medlemsstaternas nationella rätt. Detta gäller bestämmelserna i artikel 9.2 b (arbetsrätt m.m.), g (viktigt allmänt intresse), h (hälso- och sjukvård m.m.), i (folkhälsa) och j (arkiv, forskning och statistik) samt artikel 9.3. Utredningen bedömer att dessa hänvisningar i vissa fall innebär att undantagen i sig bör föreskrivas i nationell rätt, antingen i generell eller i sektorsspecifik reglering. *Pensionsmyndigheten* ifrågasätter den bedömningen.

Det är som utredningen påpekar inte helt klart vilken innebörd hänvisningarna till och kraven på unionsrätten och den nationella rätten har eller vilken betydelse det har att de utformats på olika sätt. Enligt regeringens mening är det dock uppenbart att det vid behandling av känsliga personuppgifter i de situationer som beskrivs i nämnda bestämmelser krävs ett annat stöd i rättsordningen, utöver det som dataskyddsförordningen ger. De särskilda krav som i respektive punkt ställs på det rättsliga stödet för behandlingen måste nämligen vara uppfyllda för att undantagen i artikel 9.2 ska vara tillämpliga. Dessa krav går utöver de som ställs på rättslig grund enligt artikel 6 i dataskyddsförordningen. Tröskeln för att den personuppgiftsansvarige ska få behandla känsliga personuppgifter är således högre än den som gäller för behandling av andra personuppgifter i samma situation. Detta innebär dock inte att undantagen i sig måste genomföras i svensk rätt för att vara tillämpliga. Vidare är innebörden av kravet på att behandlingen ska vara nödvändig, som *Förvaltningsrätten i Stockholm* efterfrågar förtydliganden om, enligt regeringens bedömning densamma i artikel 9 som i artikel 6, se avsnitt 8.1.

Det bör noteras att flera av undantagsbestämmelserna i artikel 9.2 inte innehåller någon hänvisning till nationell rätt, närmare bestämt de som anges i artikel 9.2 c, d, e och f. Dessa undantag gäller vid behandling som sker för att skydda en persons grundläggande intressen (c), inom vissa icke vinstdrivande organ (d), då personuppgifterna har offentliggjorts av den registrerade (e) respektive i samband med rättsliga anspråk eller i dömande verksamhet (f). Eftersom det är uppenbart att dessa bestämmelser inte föranleder några nationella författningsåtgärder behandlas de inte här. I den utsträckning det inte framkommer något annat i förordningen eller genom EU-domstolens praxis, framstår det dock som naturligt att dessa undantagsbestämmelser tolkas i linje med den praxis som utvecklats enligt motsvarande bestämmelser i dataskyddsdirektivet och personuppgiftslagen.

Regeringen anser inte att det finns skäl att, som utredningen föreslår, införa någon allmän upplysningsbestämmelse avseende behandling av känsliga personuppgifter.

Överväganden och förslag när det gäller behandling av känsliga personuppgifter för arkivändamål av allmänt intresse och statistiska ändamål finns i avsnitt 14.

10.2 Den registrerades samtycke

Regeringens bedömning: Det bör inte införas något undantag från bestämmelsen om att känsliga personuppgifter får behandlas med stöd av den registrerades uttryckliga samtycke.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna har inte gett uttryck för någon annan uppfattning.

Skälen för regeringens bedömning: I artikel 9.2 a i dataskyddsförordningen finns en möjlighet för medlemsstaterna att föreskriva att den registrerade inte kan samtycka till behandling av känsliga personuppgifter. Bestämmelsen motsvarar artikel 8.2 a i dataskyddsdirektivet. Vid

införandet av personuppgiftslagen ansåg regeringen att det inte fanns något integritetsskyddsintresse som gjorde det befogat att förbjuda en behandling som den registrerade och den personuppgiftsansvarige var överens om (prop. 1997/98:44 s. 69). Det infördes därför varken någon sådan bestämmelse i lag eller någon möjlighet för regeringen eller Datainspektionen att föreskriva om förbud mot behandling trots den registrerades samtycke. Utredningen anser att det inte heller nu bör införas ett förbud mot behandling trots den registrerades samtycke.

Regeringen ansluter sig till utredningens bedömning i denna fråga, som inte heller ifrågasätts av remissinstanserna. Den registrerades uttryckliga samtycke bör alltså även fortsättningsvis medföra att känsliga personuppgifter får behandlas. Att behandling av känsliga personuppgifter får ske då den registrerade har lämnat sitt samtycke framgår direkt av artikel 9.2 a och behöver inte föreskrivas i nationell rätt. Det innebär att någon nationell reglering inte bör införas på grund av artikel 9.2 a.

10.3 Arbetsrätt, social trygghet och socialt skydd

Regeringens förslag: Känsliga personuppgifter får behandlas om det är nödvändigt för att den personuppgiftsansvarige eller den registrerade ska kunna fullgöra sina skyldigheter och utöva sina särskilda rättigheter inom arbetsrätten och inom områdena social trygghet och socialt skydd. Personuppgifter som behandlas med stöd av detta undantag får lämnas ut till tredje part endast om det inom arbetsrätten eller inom områdena social trygghet och socialt skydd finns en skyldighet för den personuppgiftsansvarige att göra det eller om den registrerade uttryckligen har samtyckt till utlämnandet.

Utredningens förslag överensstämmer i sak med regeringens. I utredningens förslag anges dock inte områdena social trygghet och socialt skydd uttryckligen i bestämmelsen.

Remissinstanserna: En majoritet av remissinstanserna tillstyrker förslaget eller har inga synpunkter på det. *Centrala studiestödsnämnden* anser att det är klokt att inta en försiktig hållning och inte föreslå någon reglering på områdena social trygghet och socialt skydd. *Uppsala universitet* ifrågasätter i stället utredningens resonemang och anser att antagandet att den sociala trygghetslagstiftningen ligger långt bort från arbetsrätten är olyckligt och riskerar att skapa fel slutsatser om när och hur arbetsgivare får behandla personuppgifter. *Malmö kommun* och *Piteå kommun* anser att det är oklart om begreppet social trygghet och socialt skydd ska ha den EU-rättsliga innebörd som utredningen menar. *Svensk Försäkring* påpekar att gruppförsäkringar och i de flesta fall även tjänstepensionerna tillhandahålls av försäkringsföretag, som behöver behandla känsliga personuppgifter för att kunna tillhandahålla det avsedda försäkringsskyddet. *Pensionsmyndigheten* avstyrker förslaget och anser att det inte finns något i förordningstexten som ger skäl för nationella regler. *Dataskydd.net* avstyrker förslaget och anser att artikel 9.2 inte kan kringgås annat än genom lagstiftning som ger behandlingen en rättslig grund, vilket i så fall sker i annan lagstiftning än dataskyddslagen. Flera remiss-

instanser, bl.a. *Svensk Handel* och *Svenskt Näringsliv,* har synpunkter på hur bestämmelsen om utlämnande till tredje part bör tolkas och tillämpas.

Skälen för regeringens förslag

I artikel 9.2 b i dataskyddsförordningen föreskrivs ett undantag från förbudet mot behandling av känsliga personuppgifter på arbetsrättens område. Undantaget motsvaras delvis av artikel 8.2 b i dataskyddsdirektivet, som har genomförts i svensk rätt genom 16 § första stycket a PUL. Förordningens undantag är dock vidare och avser behandling som är nödvändig för att både den personuppgiftsansvarige och den registrerade ska kunna fullgöra sina rättigheter och skyldigheter inom arbetsrätten. Vidare omfattar bestämmelsen i förordningen även områdena social trygghet och socialt skydd. Undantaget gäller i den omfattning behandlingen är tillåten enligt nationell rätt eller ett kollektivavtal och under förutsättning att lämpliga skyddsåtgärder som säkerställer den registrerades grundläggande rättigheter och intressen fastställs.

Termen arbetsrätt har vid tillämpningen av personuppgiftslagen getts en vid tolkning som innebär att i stort sett alla skyldigheter och rättigheter för arbetsgivare beträffande de anställda och deras organisationer innefattas, såsom exempelvis behandling i samband med sjuklön och rehabilitering av arbetstagare. Även skyldigheter och rättigheter för fackliga organisationer i förhållande till arbetsgivare och deras organisationer omfattas.

Utredningen anser att det inte är helt klart vad som avses med begreppen social trygghet och socialt skydd i artikel 9.2 b, men konstaterar att sociallagstiftning och den lagstiftning som återfinns på socialförsäkringsområdet sakligt sett tycks ligga långt ifrån arbetsrätten. Med tanke på det sammanhang där begreppen förekommer bedömer utredningen att avsikten sannolikt i stället är att reglera behandling som är nödvändig för att arbetsgivare, fackförbund eller arbetsgivarorganisationer ska kunna erbjuda eller förmedla pensioner och försäkringar med anknytning till den registrerades anställning eller yrkesliv, såsom tjänstepensioner och olika typer av gruppförsäkringar. Eftersom sådan behandling i många fall ändå kan ske med stöd av undantaget som rör arbetsrätten, undantaget som rör viktiga allmänna intressen eller med stöd av samtycke, ser utredningen inte behov av att införa denna del av artikel 9.2 b i dataskyddslagen.

Uppsala universitet ifrågasätter utredningens bedömning i denna del. Universitetet menar att begreppen social trygghet och socialt skydd har en viss innebörd enligt EU-rätten samt att det är avsett att vara ett vitt begrepp. Utredningens antagande om att den sociala trygghetslagstiftningen ligger långt bort från arbetsrätten är enligt universitet olyckligt och riskerar att skapa fel slutsatser om när och hur arbetsgivare får behandla personuppgifter.

Enligt regeringens bedömning torde det stå klart att bestämmelsen i artikel 9.2 b gör det möjligt att behandla även känsliga personuppgifter när det är nödvändigt för att i vart fall arbetsgivare, arbetstagare, fackliga organisationer och arbetsgivarorganisationer ska kunna fullgöra sina skyldigheter eller utöva sina rättigheter med koppling till arbetslivet. Det är således inte bara behandling av personuppgifter som har sin rättsliga

grund i arbetsrätten, i snäv bemärkelse, som omfattas. Bestämmelsen bör, precis som 16 § PUL, även kunna tillämpas vid behandling av personuppgifter som en arbetsgivare utför som en följd av lagstiftningen på socialförsäkringsområdet, t.ex. i samband med en arbetstagares sjukdom och rehabilitering. Det kan därför ifrågasättas om det tillägg som gjorts i dataskyddsförordningen avseende områdena social trygghet och social omsorg innebär någon egentlig förändring jämfört med vad som gäller enligt personuppgiftslagen. För närvarande går det dock inte att dra några helt säkra slutsatser om begreppens innebörd. Som Uppsala universitet påpekar har begreppen en unionsrättslig innebörd och denna kommer efter hand att klargöras genom bl.a. EU-domstolens praxis. Det kan därför inte uteslutas att begreppen har en vidare innebörd än vad som följer av utredningens bedömning.

En förutsättning för att behandlingen ska omfattas av undantaget i artikel 9.2 b är att den är tillåten enligt gällande rätt, t.ex. enligt kollektivavtal, och att detta rättsliga stöd innehåller bestämmelser om lämpliga skyddsåtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen. Detta innebär dock inte att undantaget i sig måste genomföras i svensk rätt för att vara tillämpligt.

Det finns inte bara en, utan många olika tänkbara rättsliga grunder för behandling av personuppgifter med koppling till arbetslivet. I de fall den rättsliga grunden är en rättslig förpliktelse eller en uppgift av allmänt intresse ska den, enligt artikel 6.3 första stycket i dataskyddsförordningen, vara fastställd i enlighet med unionsrätten eller den nationella rätten. Sådana fastställda förpliktelser och uppgifter för exempelvis arbetsgivare förekommer i Sverige i kollektivavtal och arbetsrättslig lagstiftning, men också på andra områden, t.ex. i socialförsäkringsbalken, lagen (1991:1047) om sjuklön och diskrimineringslagen (2008:567).

Behov av att behandla också känsliga personuppgifter i dessa sammanhang förekommer i alla sektorer av samhället. Det finns inte någon sektorsspecifik reglering som på ett övergripande plan tillgodoser förordningens krav på skyddsåtgärder. Motsvarande krav på skyddsåtgärder i dataskyddsdirektivet har i stället tillgodosetts genom bestämmelsen i 16 § första stycket a samt andra stycket PUL.

För att möjliggöra sådan nödvändig behandling som avses i artikel 9.2 b och samtidigt tillgodose kravet på skyddsåtgärder anser regeringen, till skillnad från bl.a. *Pensionsmyndigheten*, att det krävs en generell reglering i svensk rätt även fortsättningsvis. Med avvikelse från utredningens förslag bör denna uttryckligen omfatta även områdena social trygghet och socialt skydd. Den svenska bestämmelsen skulle annars, mot bakgrund av att förordningen nämner dessa områden särskilt, kunna uppfattas som snävare än avsett.

En begränsning av möjligheten att lämna ut uppgifter till utomstående, i likhet med vad som gäller enligt 16 § andra stycket PUL, framstår som en i sammanhanget effektiv och lämplig skyddsåtgärd. Känsliga personuppgifter som behandlas med stöd av detta undantag bör således få lämnas ut till tredje part bara om det inom arbetsrätten eller inom områdena social trygghet och socialt skydd finns en uttrycklig skyldighet för den personuppgiftsansvarige att göra det eller den registrerade har samtyckt till utlämnandet. De synpunkter som bl.a. *Svenskt Näringsliv* framför angående behovet av att även i andra fall än dessa lämna ut upp-

gifter till utomstående föranleder inte regeringen att göra någon annan bedömning än utredningen i fråga om den generella reglering som det nu är fråga om. Den skyldighet att lämna ut personuppgifter som avses i 16 § andra stycket PUL ska följa av lagstiftning, myndighetsbeslut eller av ett muntligt eller skriftligt avtal (jfr prop. 1997/98:44 s. 124). Detsamma bör gälla även fortsättningsvis. På motsvarande sätt bör den praxis som finns kring tillämpningen av 16 § andra stycket PUL kunna vara vägledande även vid tillämpningen av bestämmelsen i dataskyddslagen.

Det förtjänar att poängteras att den föreslagna bestämmelsen inte ersätter vare sig artikel 6 eller artikel 9.2 b i dataskyddsförordningen. De skyldigheter och rättigheter som gör behandlingen nödvändig, och därmed utgör rättslig grund, måste fastställas någon annanstans än i dataskyddslagen. Vidare kan de särskilda krav som ställs i artikel 9.2 b vara uppfyllda även genom andra bestämmelser än den föreslagna. Behandling av känsliga personuppgifter kan alltså ske med stöd av artikel 9.2 b även i andra fall, nämligen om behandlingen är tillåten enligt kollektivavtal eller enligt annan författning än dataskyddslagen, under förutsättning att lämpliga skyddsåtgärder fastställts.

Många gruppförsäkringar och kanske särskilt flera av de som har anknytning till arbetslivet eller som följer av kollektivavtal kan fylla en viktig funktion inom området social trygghet och socialt skydd (jfr prop. 2003/04:150 s. 314 och 343). Den föreslagna bestämmelsen skulle därför kunna vara tillämplig även för de som tillhandahåller eller administrerar sådana försäkringar. Bestämmelsen utgör inte heller någon inskränkning av de möjligheter att behandla känsliga personuppgifter som följer av andra undantagsbestämmelser i artikel 9.2 i dataskyddsförordningen. Flera undantagsbestämmelser kan vara tillämpliga samtidigt. Således kommer exempelvis försäkringsföretag även i fortsättningen att, med stöd av artikel 9.2 f, kunna behandla känsliga personuppgifter när detta är nödvändigt till följd av avtal med fackliga organisationer om gruppförsäkring för deras medlemmar (jfr prop. 1997/98:44 s. 125). På motsvarande sätt kan det vara nödvändigt för t.ex. en arbetsgivare att med stöd av artikel 9.2 f lämna ut uppgifter till en advokat eller annan rådgivare, för att kunna göra gällande eller försvara rättsliga anspråk i arbetsrättsliga ärenden.

10.4 Viktigt allmänt intresse

Regeringens förslag: Myndigheter och andra som omfattas av offentlighetsprincipen får behandla känsliga personuppgifter, om uppgifterna har lämnats till den personuppgiftsansvarige och behandlingen krävs enligt lag. Dessutom får en myndighet behandla känsliga personuppgifter, om det är nödvändigt för handläggningen av ett ärende. Vidare får känsliga personuppgifter behandlas av en myndighet i enstaka fall, om behandlingen är nödvändig med hänsyn till ett viktigt allmänt intresse och inte innebär ett otillbörligt intrång i den registrerades personliga integritet.

Vid behandling som sker enbart med stöd av de nämnda grunderna, är det förbjudet att utföra sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter.

Regeringen får meddela ytterligare föreskrifter om sådan behandling av känsliga personuppgifter som är nödvändig med hänsyn till ett viktigt allmänt intresse.

Utredningens förslag överensstämmer i huvudsak med regeringens. Utredningen föreslår att myndigheter ska få behandla känsliga personuppgifter i löpande text om uppgifterna har lämnats i ett ärende eller är nödvändiga för handläggningen av det. Dessutom innebär utredningens förslag att myndigheter i enstaka fall ska få behandla känsliga personuppgifter om det är absolut nödvändigt för ändamålet med behandlingen och behandlingen inte innebär ett otillbörligt intrång i den registrerades personliga integritet. Slutligen föreslår utredningen ett absolut sökförbud samt att bemyndigandet ska ha en annan språklig utformning.

Remissinstanserna: En majoritet av remissinstanserna tillstyrker förslaget eller har inga synpunkter på det. *Socialstyrelsen*, *Malmö kommun*, *Piteå kommun* och *Västra Götalands läns landsting* anser att den generella regleringen behövs bl.a. för att täcka in behandling som inte omfattas av någon sektorsspecifik reglering. *Kronofogdemyndigheten* anser att utredningens förslag är viktiga för att myndigheten ska kunna behandla personuppgifter som är nödvändiga i verksamheten. *Lunds universitet* konstaterar att förslaget i princip följer Informationshanteringsutredningens förslag och anser att detta är lämpligt, men skulle inte heller motsätta sig en viss utvidgning av myndigheternas möjligheter att hantera personuppgifter i allmänt intresse. *Diskrimineringsombudsmannen* påpekar att vad som anses vara viktiga allmänna intressen varierar över tid och är beroende av samhällsutvecklingen samt anser att myndigheters möjligheter till behandling av känsliga personuppgifter i enstaka fall ska begränsas särskilt. *Riksrevisionen* anser att utredningens uttalande om att begränsningen till löpande text inte behöver utesluta att handlingar med ostrukturerade känsliga personuppgifter lagras elektroniskt i ärendehanteringssystem eller liknande behöver utvecklas. Vidare menar Riksrevisionen att det vore önskvärt att ett sådant undantag från förbudet att behandla känsliga personuppgifter kommer till uttryck i lagen. Riksrevisionen påpekar vidare att känsliga personuppgifter kan behöva behandlas på annat sätt än i löpande text för att utföra lagstadgad revision. *Barnombudsmannen* ser ett behov av förtydligande i författningstexten som klargör och säkerställer att myndighetens behandling av

känsliga personuppgifter kan ske i den faktiska verksamheten. *Skatteverket* anser att det är oklart vad förslaget om undantag från förbudet att behandla känsliga personuppgifter i enstaka fall ska omfatta. Piteå kommun anser att kravet på absolut nödvändighet för ändamålet skulle kunna mildras och förordar i stället en skrivning som ger möjlighet till behandling liknande den som medges enligt 5 a § PUL. *Datainspektionen* avstyrker förslaget och anser att bestämmelsen bör utformas så att det klart framgår att behandling av känsliga personuppgifter endast är tillåten om behandlingen är nödvändig med hänsyn till ett viktigt allmänt intresse. Om denna särskilda förutsättning för behandlingen inte framgår finns enligt Datainspektionen risk för att myndigheter vilseleds av formuleringen, särskilt som det inte finns någon egentlig begränsning av vad myndigheter kan behandla som ärende. Datainspektionen håller med utredningen om att myndigheters hantering av inkomna handlingar torde utgöra ett sådant viktigt allmänt intresse. För att uppnå det som utredningen har avsett och som den har bedömt proportionerligt krävs att förslaget i den delen begränsas till den lagstiftning som reglerar myndigheters och likställda organs hantering av inkomna handlingar. Att införa ett nytt begrepp, absolut nödvändigt, riskerar enligt Datainspektionen att leda till förvirring hos den enskilde personuppgiftsansvarige och en felaktig tillämpning av dataskyddsregleringen. Även *Kungliga tekniska högskolan* anser att begreppet absolut nödvändigt har språkliga likheter med begreppet nödvändigt och att en begreppsförvirring är oundviklig. *Förvaltningsrätten i Stockholm* ifrågasätter varför nödvändighetskravet inte finns med i vissa av förslagen. Lunds universitet anför, angående det föreslagna undantaget för behandling som krävs enligt lag, att det bör framgå tydligare av lagtexten om avsikten är att knyta undantaget till offentlighetsprincipen. *Pensionsmyndigheten* anser inte att det är självklart att förordningen ska tolkas så att det finns ett behov av att i dataskyddslagen eller i annan nationell lagstiftning ta in bestämmelser om undantag från förbudet att behandla känsliga personuppgifter. Pensionsmyndigheten anser att det bör analyseras ytterligare om det är det viktiga allmänna intresset, snarare än behandlingen, som ska regleras i nationell rätt. Vidare anser Pensionsmyndigheten att den föreslagna bestämmelsen rörande behandling i löpande text kan bli svår att tillämpa för myndigheter som har helt automatiserade handläggningsflöden och anser därför att den bör göras teknikneutral. Pensionsmyndigheten vill också framhålla att den lagtekniska utformningen, som innebär att bestämmelserna avgränsats till uppgifter som lämnats i ett ärende eller till myndigheten, gör att det inte är möjligt att tillämpa bestämmelsen när behandling av känsliga personuppgifter sker i myndigheters s.k. egna utrymmen. Likartade synpunkter angående myndigheternas egna utrymmen har lämnats av *Bolagsverket* och *Sveriges advokatsamfund*. *Dataskydd.net* avstyrker förslaget och anser att artikel 9.2 inte kan kringgås annat än genom lagstiftning som ger behandlingen en rättslig grund, vilket i så fall sker i annan lagstiftning än i dataskyddslagen. *Hovrätten för Västra Sverige* anser att det är positivt att utredningen föreslår att myndigheter inte får använda sökbegrepp som avslöjar känsliga personuppgifter. *Domstolsverket* anser att ett sökförbud som utformats i enlighet med utredningens förslag är lätt att tillämpa och därmed leder till tydlighet och enkelhet. Domstolsverket påpekar dock att det vid behandling för arkivändamål av

allmänt intresse inte finns något sökförbud, vilket torde få till följd att det sökförbud som gäller för myndigheters personuppgiftsbehandling upphör i samband med att uppgifter arkiveras. *Polismyndigheten* tillstyrker förslaget om generellt sökförbud men framhåller att det behövs ett undantag för sökningar på känsliga personuppgifter som sker i registervårdande syfte. *Säkerhets- och integritetsskyddsnämnden* ifrågasätter utformningen av det föreslagna sökförbudet och anser att dess ordalydelse i praktiken förhindrar all användning av sökbegrepp, vilket bl.a. kan omöjliggöra en effektiv registervård och tillsyn. *Migrationsverket* anser att det, utifrån ett integritetsperspektiv, är bra att det föreslås ett sökförbud gällande känsliga personuppgifter, men påpekar att det medför en risk för att viss nödvändig personuppgiftsbehandling inte kan genomföras. Migrationsverket anser att sökning, även gällande känsliga personuppgifter, borde tillåtas med förbehållet att uppgifterna endast får tas fram för helt avidentifierad statistik. *Skatteverket* anser att det skulle underlätta om sökbegränsningarna utformas på samma sätt i dataskyddslagen och brottsdatalagen. *Specialpedagogiska skolmyndigheten* påpekar att sökförbudet kan leda till problem för specialskolan när det gäller att ta fram verksamhetsstatistik. *Transportstyrelsen* anser att det, om det införs ett sökförbud för känsliga personuppgifter, bör övervägas undantag för myndigheters sökningar i verksamhetssystem där syftet är att följa upp och kvalitetssäkra den egna verksamheten. Piteå kommun ser stora administrativa svårigheter med att leva upp till ett förbud mot att använda sökbegrepp som avslöjar känsliga personuppgifter. Detta förslag riskerar enligt kommunen att bli kostnadsdrivande för kommunerna utan tydlig nytta. Sveriges advokatsamfund anser att den föreslagna sökbegränsningen bör anpassas till den service som myndigheter ger åt privatpersoner.

Skälen för regeringens förslag

Begreppet viktigt allmänt intresse

Av artikel 9.2 g framgår att förbudet mot behandling av känsliga personuppgifter inte gäller om behandlingen är nödvändig av hänsyn till ett viktigt allmänt intresse, på grundval av unionsrätten eller medlemsstaternas nationella rätt, vilken ska stå i proportion till det eftersträvade syftet, vara förenligt med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande intressen. Bestämmelsen motsvarar artikel 8.4 i dataskyddsdirektivet.

En första förutsättning för att detta undantag ska vara tillämpligt är att behandlingen är nödvändig med hänsyn till ett viktigt allmänt intresse. Vad som är ett allmänt intresse respektive ett viktigt allmänt intresse är dock inte definierat i vare sig dataskyddsdirektivet eller dataskyddsförordningen, och begreppens innebörd har inte heller utvecklats närmare av EU-domstolen.

I förordningen används begreppet viktigt allmänt intresse, förutom i artikel 9.2 g, även i artikel 17 angående folkhälsoområdet och i artikel 23.1 e angående unionens eller en medlemsstats viktiga ekonomiska eller finansiella intressen, däribland penning-, budget- eller skattefrågor, folkhälsa och social trygghet. I skäl 19 andra stycket anges

att när privata organs behandling av personuppgifter omfattas av förordningens tillämpningsområde, bör förordningen ge medlemsstaterna möjlighet att, under särskilda villkor, i lag begränsa vissa skyldigheter och rättigheter, om en sådan begränsning utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle för att skydda särskilda viktiga intressen, däribland allmän säkerhet samt förebyggande, förhindrande, utredning, avslöjande och lagföring av brott eller verkställande av straffrättsliga påföljder eller skydd mot samt förebyggande och förhindrande av hot mot den allmänna säkerheten. Detta är enligt samma skäl exempelvis relevant i samband med bekämpning av penningtvätt eller verksamhet vid kriminaltekniska laboratorier. I skäl 112 anges internationella utbyten av uppgifter mellan konkurrensmyndigheter, skatte- eller tullmyndigheter, finanstillsynsmyndigheter, socialförsäkringsmyndigheter eller hälsovårdsmyndigheter, t.ex. vid kontaktspårning för smittsamma sjukdomar eller för att minska och/eller undanröja dopning inom idrott, som exempel på viktiga allmänintressen.

Det är, som utredningen påpekar, svårt att på ett generellt plan definiera vad som skiljer ett allmänt intresse från ett viktigt allmänt intresse. Enligt regeringens bedömning torde det dock stå klart att verksamhet som innefattar myndighetsutövning utgör ett viktigt allmänt intresse. När det gäller myndigheters behandling måste det enligt regeringens mening också anses utgöra ett viktigt allmänt intresse att svenska myndigheter, även utanför området för myndighetsutövning, kan bedriva den verksamhet som tydligt faller inom ramen för deras befogenheter på ett korrekt, rättssäkert och effektivt sätt.

Av de exempel som ges i förordningen framgår dock att också viss verksamhet som bedrivs av privata aktörer kan omfattas av begreppet viktigt allmänt intresse. Utrymmet för att privata aktörer ska kunna tillämpa artikel 9.2 g behandlas dock inte i utredningens betänkande och omfattas inte heller av detta lagstiftningsärende.

Särskilda krav ställs på det rättsliga stödet

En andra förutsättning för att undantaget i artikel 9.2 g ska vara tillämpligt är att behandlingen sker på grundval av unionsrätten eller medlemsstaternas nationella rätt, vilken ska stå i proportion till det eftersträvade syftet. Enligt regeringens bedömning innebär detta att den rättsliga grunden för behandlingen ska vara någon av de som avses i artikel 6.1 c eller e, dvs. en rättslig förpliktelse, en uppgift av allmänt intresse eller myndighetsutövning som har stöd i rättsordningen på det sätt som beskrivs i avsnitt 8.

För att behandling av känsliga personuppgifter ska få ske ställs emellertid särskilda krav på det rättsliga stödet. Detta måste vara förenligt med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande intressen. Det kan konstateras att dessa krav på det rättsliga stödet motsvarar kraven för att begränsa de rättigheter som skyddas av EU:s stadga om de grundläggande rättigheterna. I artikel 52 i stadgan anges att varje begränsning i utövandet av de rättigheter och friheter som erkänns i denna stadga ska vara föreskriven i lag och förenlig med det väsentliga innehållet i dessa rättigheter och friheter.

Vad som utgör det väsentliga innehållet i rätten till dataskydd definieras inte i dataskyddsförordningen. Regeringen har dock svårt att föreställa sig en rättslig grund för behandling av personuppgifter som uppfyller kraven i artikel 6, men som ändå inte är förenlig med det väsentliga innehållet i rätten till dataskydd. Om grunden för behandlingen inte är förenlig med det väsentliga innehållet i rätten till dataskydd torde den inte utgöra en godtagbar rättslig grund för behandling av personuppgifter över huvud taget. Det kan därför ifrågasättas om tillägget i artikel 9.2 g utgör ett krav som går utöver de krav som gäller enligt artikel 6 och som måste vara uppfyllda vid all behandling av personuppgifter i allmänt intresse.

Däremot tillkommer enligt artikel 9.2 g ett krav på att gällande rätt innehåller bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande intressen. Detta krav överensstämmer med det som har gällt även enligt dataskyddsdirektivet och innebär således ingen ny begränsning av möjligheten att behandla känsliga personuppgifter. Det innebär inte heller att undantaget i sig måste genomföras i svensk rätt för att vara tillämpligt.

Det behövs en generell reglering avseende myndigheters behandling

För att myndigheter ska kunna bedriva sin verksamhet är det ofta nödvändigt att behandla känsliga personuppgifter och i många fall sker behandlingen i den registrerades eget intresse. Det finns därför ett behov av en tydlig reglering som tillåter viss behandling av känsliga personuppgifter hos myndigheterna. I många fall finns sådana bestämmelser i sektorsspecifika författningar om behandling av personuppgifter. Det finns också bestämmelser som tillåter behandling av känsliga personuppgifter på ett mer indirekt sätt, t.ex. i form av bestämmelser som anger att uppgifter eller handlingar ska överlämnas till andra myndigheter eller till enskilda som begär det. Det behov av att behandla känsliga personuppgifter som därutöver finns hos myndigheter är i dag tillgodosett genom att viss behandling är tillåten genom den s.k. missbruksregeln i 5 a § PUL och enligt 8 § PUF.

Dataskyddsdirektivets krav på skyddsåtgärder har i svensk rätt ofta ansetts tillgodosett genom att uppgifterna omfattas av bestämmelser om sekretess. Det har också ansetts utgöra en skyddsåtgärd att bara tillåta behandling av känsliga personuppgifter som inte innefattar ett missbruk av personuppgifterna (prop. 2005/06:173 s. 34).

Missbruksregeln i 5 a § PUL anger att flertalet bestämmelser i personuppgiftslagen inte ska 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. Bestämmelsen innebär bl.a. att förbudet mot behandling av känsliga personuppgifter inte gäller vid sådan ostrukturerad behandling. I stället gäller en allmän begränsning om att behandling inte får utföras om den innebär en kränkning av den registrerades personliga integritet. Bestämmelsen är enligt förarbetena avsedd att gälla t.ex. vid behandling av personuppgifter i löpande text i ordbehandlingsprogram, i e-post eller på internet (prop. 2005/06:173 s. 58).

Enligt 8 § PUF får känsliga personuppgifter behandlas av en myndighet i löpande text, om uppgifterna har lämnats i ett ärende eller är nödvändiga för handläggningen av det. Bestämmelsen möjliggör t.ex. att känsliga personuppgifter får finnas i skälen till ett beslut, när det krävs för att uppfylla kraven på att beslut ska innehålla de skäl som bestämt utgången. Dessutom har bestämmelsen ansetts ge stöd för att uppgifter behandlas i ärendehanteringssystem, då de förekommer i handlingar med löpande text (SOU 2015:39 s. 306). Den formulering som används i 8 § PUF har däremot inte ansetts omfatta s.k. faktisk verksamhet som en myndighet bedriver (jfr Lagrådets yttrande över förslaget till lag om behandling av personuppgifter inom socialtjänsten, prop. 2000/01:80 s. 272), t.ex. rådgivning och annan service, uppföljning eller olika former av samverkan utan ärendeanknytning. Vid faktisk verksamhet är det således bara 5 a § PUL som kan tillämpas, om sektorsspecifik reglering saknas.

Det kan enligt regeringens mening inte råda något tvivel om att det är ett viktigt allmänt intresse att myndigheterna kan sköta sitt uppdrag på ett korrekt, rättssäkert och effektivt sätt. Det gäller även, som bl.a. *Barnombudsmannen* påpekar, i den faktiska verksamheten. Missbruksregeln i 5 a § PUL har dock ingen motsvarighet i dataskyddsförordningen. Det kan inte heller tas för givet att det för all offentlig verksamhet redan finns sådana lämpliga och särskilda åtgärder som krävs enligt artikel 9.2 g i dataskyddsförordningen för att känsliga personuppgifter ska få behandlas. Regeringen bedömer därför, till skillnad från bl.a. *Pensionsmyndigheten*, att det behövs särskilda bestämmelser i dataskyddslagen som är tillämpliga för alla myndigheter och som uppfyller kraven i artikel 9.2 g i dataskyddsförordningen.

Pensionsmyndigheten, *Bolagsverket* och *Sveriges advokatsamfund* påpekar att det inte är möjligt att tillämpa de bestämmelser som utredningen föreslår när känsliga personuppgifter behandlas i myndigheters s.k. egna utrymmen. Regeringen kan dock konstatera att de särskilda frågeställningar som rör sådan behandling inte föranleds av dataskyddsförordningen. Därmed behandlas de inte i detta lagstiftningsärende.

Behandling som krävs enligt lag

Viss behandling av känsliga personuppgifter är oundviklig i myndigheternas verksamhet som en direkt följd av exempelvis offentlighets- och sekretesslagens och förvaltningslagens krav, såsom krav på diarieföring och skyldighet att ta emot e-post. Samma skyldigheter gäller i viss utsträckning för vissa andra organ än myndigheter, som en följd av att dessa organ jämställs med myndigheter enligt offentlighets- och sekretesslagen. Utredningen föreslår mot denna bakgrund en bestämmelse om att myndigheter och andra organ som omfattas av offentlighetsprincipen får behandla känsliga personuppgifter som har lämnats till myndigheten eller organet om behandlingen krävs enligt lag.

Den grundlagsfästa rätten att ta del av allmänna handlingar måste enligt regeringens mening anses utgöra ett viktigt allmänt intresse. Ordning och reda bland allmänna handlingar är en förutsättning för att handlingsoffentligheten ska fungera och fylla sitt syfte. Den hantering av allmänna handlingar som krävs enligt svensk rätt är därför motiverad

med hänsyn till ett viktigt allmänt intresse. En stor del av denna hantering sker i den elektroniska miljön och medför behandling av personuppgifter.

Den nödvändiga behandling av personuppgifter som sker vid hanteringen av allmänna handlingar har rättslig grund i svensk rätt, framför allt i offentlighets- och sekretesslagen, arkivlagstiftningen och förvaltningslagen. Denna lagstiftning innehåller lämpliga och särskilda åtgärder som skyddar enskildas integritet, t.ex. i form av sekretess, rätt till partsinsyn och föreskrifter om informationssäkerhet och gallring. Enligt regeringens bedömning kan därmed även känsliga personuppgifter behandlas då det är nödvändigt i dessa sammanhang, med stöd av artikel 9.2 g i dataskyddsförordningen.

För att det inte ska råda något tvivel om att denna nödvändiga behandling är tillåten också efter den 25 maj 2018 bör dataskyddslagen innehålla en uttrycklig bestämmelse som tydliggör detta. Enligt regeringens mening saknas det skäl att, som *Datainspektionen* och *Lunds universitet* förordar, tydligare än utredningens förslag koppla bestämmelsen till den behandling som sker som en följd av offentlighetsprincipen. Den föreslagna formuleringen, som innebär att behandling är tillåten endast om den krävs enligt lag i kombination med att bestämmelsen endast avser uppgifter som har lämnats till myndigheten, utgör enligt regeringens bedömning en tillräckligt tydlig begränsning av bestämmelsens tillämpningsområde. Således bör det av dataskyddslagen framgå att myndigheter och andra som omfattas av offentlighetsprincipen får behandla känsliga personuppgifter, om uppgifterna har lämnats till myndigheten och behandlingen krävs enligt lag.

Det bör noteras att ett utlämnande av en allmän handling som sker på begäran av en enskild inte sker med stöd av dataskyddsförordningen eller dataskyddslagen. Ett sådant utlämnande sker i stället med stöd av tryckfrihetsförordningen, som enligt artikel 86 och den bestämmelse som föreslås i avsnitt 7.1 har företräde framför dataskyddsförordningen. Detta gäller även om den allmänna handlingen innehåller känsliga personuppgifter.

Behandling som är nödvändig för handläggningen av ett ärende

Utredningen föreslår att myndigheter ska få behandla känsliga personuppgifter i löpande text om uppgifterna har lämnats i ett ärende eller är nödvändiga för handläggningen av det. Förslaget motsvarar 8 § PUF. Regeringen kan dock konstatera att uppgifter som har lämnats i ett ärende, men som inte är nödvändiga för handläggningen av ärendet, inte bör behandlas i större utsträckning än vad som krävs enligt lag. Sådan behandling är tillåten enligt vad som anförs ovan. Stödet för denna behandling behöver inte upprepas i den bestämmelse som nu övervägs.

Som framgår av avsnitt 8 är myndighetsutövning och övriga uppgifter av allmänt intresse som myndigheter har befogenhet att utföra alltid fastställda i enlighet med svensk rätt. Behandling av personuppgifter kan därmed ske på denna rättsliga grund. Enligt regeringens bedömning står det klart att det också är ett *viktigt* allmänt intresse att myndigheternas ärendehandläggning kan ske på ett effektivt och rättssäkert sätt. *Datainspektionen* anser att det inte finns någon egentlig begränsning av

vad myndigheter kan behandla som ärende och anser att bestämmelsen bör utformas så att det klart framgår att behandling av känsliga personuppgifter endast är tillåten om behandlingen är nödvändig med hänsyn till ett viktigt allmänt intresse. Regeringens uppfattning är dock att ärendebegreppet i de allra flesta fall är förhållandevis tydligt (jfr prop. 2016/17:180 s. 23–25 och s. 286). Begreppet används som avgränsning för förvaltningslagens tillämpningsområde och bör enligt regeringens mening användas även här. Bestämmelsen bör således vara tillämplig vid handläggningen av ett ärende.

Som *Förvaltningsrätten i Stockholm* påpekar innehåller utredningens förslag inget krav på att behandlingen ska vara nödvändig vid handläggningen av ett ärende. I stället anges att uppgifterna ska vara nödvändiga. Regeringen anser att det uttryck som används i artikel 9.2 g i dataskyddsförordningen, dvs. att behandlingen ska vara nödvändig, bör användas även i dataskyddslagen. Detta utgör ingen förändring i sak, eftersom det inte kan anses vara nödvändigt att behandla sådana uppgifter som i sig inte behövs. Således bör det i bestämmelsen anges att behandlingen ska vara nödvändig för handläggningen av ett ärende.

Utredningens förslag är begränsat till behandling i löpande text. Utredningen uttalar dock att denna begränsning inte bör utesluta att handlingar med ostrukturerade känsliga personuppgifter lagras elektroniskt i ärendehanteringssystem eller liknande. *Riksrevisionen* anser att detta uttalande behöver utvecklas och att det vore önskvärt att ett sådant undantag från förbudet att behandla känsliga personuppgifter kommer till uttryck i lagen. *Pensionsmyndigheten* anser att den föreslagna bestämmelsen kan bli svår att tillämpa för myndigheter som har helt automatiserade handläggningsflöden och anser därför att den bör göras teknikneutral.

Regeringen kan konstatera att den tekniska utvecklingen har lett till att de flesta ordbehandlingsprogram och e-postapplikationer, liksom dokument- och ärendehanteringssystem, innehåller sök- och sorteringsfunktioner som gör det mycket enkelt att strukturera informationen, även om detta inte varit syftet med den ursprungliga registreringen av uppgifterna. Gränsen mellan vad som utgör strukturerad och ostrukturerad behandling är således inte alltid helt lätt att dra och därmed mindre ändamålsenlig som avgränsning i fråga om vad som utgör ett otillbörligt integritetsintrång.

Som Informationshanteringsutredningen konstaterade i sitt betänkande hanteras myndigheters ärenden i dag vanligen inom ramen för ett elektroniskt ärendehanteringssystem, dvs. i en databas (SOU 2015:39 s. 306). Nödvändig behandling av känsliga personuppgifter, bl.a. i sådana system, bör enligt regeringens mening vara tillåten vid handläggningen av ett ärende oavsett om uppgifterna förekommer i löpande text eller inte. De skyddsåtgärder som omgärdar myndigheternas behandling, bl.a. genom bestämmelserna om sekretess i offentlighets- och sekretesslagen och bestämmelserna om partsinsyn m.m. i förvaltningslagen, bör i stället kompletteras med en sökbegränsning (se nedan).

Sammanfattningsvis föreslår regeringen att myndigheter ska få behandla känsliga personuppgifter om behandlingen är nödvändig för handläggningen av ett ärende.

Behandling som inte innebär ett otillbörligt intrång

Även inom ramen för myndigheters faktiska verksamhet, dvs. sådan verksamhet som inte utgör handläggning av ärenden, är behandling av känsliga personuppgifter ofta nödvändig med hänsyn till viktiga allmänna intressen. Det kan t.ex. röra sig om att myndigheten besvarar en fråga från en medborgare som via e-post uppgett känsliga personuppgifter eller att känsliga personuppgifter framkommer vid kommunikationen mellan skola och föräldrar eller inom en myndighet i samband med utvärdering av den egna verksamheten. Enligt nuvarande ordning är sådan behandling tillåten med stöd av missbruksregeln i 5 a § PUL, om behandlingen inte innebär en kränkning av den registrerades personliga integritet. Regeringen anser, mot bakgrund av vikten av att samhällets funktioner upprätthålls, att dataskyddslagen på ett likartat sätt bör ge myndigheterna ett visst utrymme för behandling av känsliga personuppgifter även i den faktiska verksamheten.

Utredningen föreslår att myndigheter i enstaka fall ska få behandla känsliga personuppgifter om det är absolut nödvändigt för ändamålet med behandlingen och behandlingen inte innebär ett otillbörligt intrång i den registrerades personliga integritet. *Datainspektionen* invänder mot användningen av begreppet absolut nödvändigt och anser, liksom *Kungliga tekniska högskolan*, att det leder till begreppsförvirring. Datainspektionen föreslår att begreppet synnerlig vikt används i stället. *Piteå kommun* anser att kravet på absolut nödvändighet för ändamålet skulle kunna mildras.

Regeringen instämmer i att användningen av olika rekvisit, vars närmare innebörd i förhållande till varandra inte är uppenbar, skulle kunna leda till vissa tillämpningssvårigheter. Det krav som gäller enligt dataskyddsförordningen, dvs. att behandlingen ska vara nödvändig, bör därför användas även i dataskyddslagen. Att bestämmelsen är avsedd att användas restriktivt bör i stället markeras genom ett snävt tillämpningsområde.

Inom myndigheternas faktiska verksamhet kan det förekomma situationer där behandling av känsliga personuppgifter inte kan anses vara nödvändig med hänsyn till ett viktigt allmänt intresse, även om behandlingen är nödvändig för något annat ändamål. Utredningens förslag innehåller dock ingen begränsning i fråga om tillåtna ändamål. Datainspektionen anser att bestämmelsen bör utformas så att det klart framgår att behandling av känsliga personuppgifter endast är tillåten om behandlingen är nödvändig med hänsyn till ett viktigt allmänt intresse. Regeringen är av samma uppfattning. Bestämmelsen bör således, för att bättre överensstämma med artikel 9.2 g i dataskyddsförordningen, avgränsas till behandling som är nödvändig med hänsyn till ett viktigt allmänt intresse. Den närmare EU-rättsliga innebörden av begreppet viktigt allmänt intresse bör överlämnas till rättstillämpningen att utveckla.

I likhet med utredningen anser regeringen att bestämmelsen bör vara tillämplig endast i enstaka fall. Denna begränsning hindrar visserligen inte att bestämmelsen tillämpas vid behandling av många personuppgifter samtidigt, så länge behandlingen sker i en viss, enstaka, situation.

Däremot motverkar den att känsliga personuppgifter behandlas slentrianmässigt i den löpande verksamheten, utan att annat författningsstöd finns.

Bestämmelsen bör utformas på ett sätt som säkerställer att det alltid finns lämpliga och särskilda åtgärder för den registrerade, på det sätt som krävs för att nödvändig behandling av känsliga personuppgifter ska vara tillåten enligt artikel 9.2 g. Till en början ska bestämmelsen bara vara tillämplig i enstaka fall, vilket i sig kan anses innebära en skyddsåtgärd. Vidare finns det i svensk rätt redan en omfattande sekretessreglering, till skydd för enskildas ekonomiska och personliga förhållanden, som i många fall utgör en tillräcklig skyddsåtgärd. Dessutom föreslås att en särskild sökbegränsning ska införas i dataskyddslagen (se nedan). En bestämmelse som reglerar möjligheten att behandla känsliga personuppgifter i myndigheternas faktiska verksamhet, bör dock innehålla ytterligare särskilda skyddsåtgärder. Det är angeläget även mot bakgrund av vad *Diskrimineringsombudsmannen* påpekar, nämligen att vad som anses vara viktiga allmänna intressen varierar över tid och är beroende av samhällsutvecklingen.

Bestämmelsen bör därför, som utredningen föreslår, innehålla ett krav på att behandlingen inte får ske om den innebär ett otillbörligt intrång i de registrerades integritet. För att avgöra om intrånget är otillbörligt måste myndigheten göra en proportionalitetsbedömning där behovet av att utföra behandlingen viktas mot de registrerades intresse av att behandlingen inte sker. Detta innebär inte att den personuppgiftsansvarige måste göra en bedömning i förhållande till varje berörd individ. Ju mindre tydligt myndighetens behov av att behandla uppgifterna är, desto större är dock sannolikheten för att de registrerades intresse typiskt sett väger tyngre och att intrånget därför bör betraktas som otillbörligt. Vid bedömningen av de registrerades intresse bör vikt läggas vid sådana aspekter som uppgifternas känslighet, behandlingens karaktär, den inställning de registrerade kan antas ha till behandlingen, den spridning uppgifterna kan komma att få och risken för vidarebehandling för andra ändamål än insamlingsändamålet. Den närmare betydelsen av begreppet otillbörligt intrång bör dock också ges utrymme att utvecklas i rättstillämpningen.

I detta sammanhang bör noteras att det vid behandling som innebär betydande intrång i den personliga integriteten och innebär övervakning eller kartläggning av den enskildes personliga förhållanden krävs särskilt lagstöd enligt 2 kap. 6 och 20 §§ RF.

Sökbegränsning

Utredningen föreslår, som en ytterligare skyddsåtgärd, att myndigheter inte ska få använda sökbegrepp som avslöjar känsliga personuppgifter. Sökförbudet är avsett att omfatta alla typer av tekniska åtgärder som innebär att uppgifter används för att strukturera eller systematisera information så att känsliga personuppgifter avslöjas. Sökförbudet har dock begränsats till att avse de fall då behandlingen sker enbart med de generella myndighetsundantagen som grund. Det innebär bl.a., som *Domstolsverket* noterar, att sökförbudet inte ska gälla vid behandling för arkivändamål av allmänt intresse (avsnitt 14).

Regeringen kan konstatera att en sökning som avslöjar och sammanställer känsliga personuppgifter är en åtgärd som i sig innebär en integritetskränkning. Företeelsen ligger nära det som ursprungligen har motiverat förbudet mot behandling av känsliga personuppgifter, nämligen möjligheten att kartlägga personer på grundval av exempelvis etnicitet eller politiska åsikter. Med en sökbegränsning uppnås därmed ett skydd av just de intressen som bestämmelserna om känsliga personuppgifter ska värna. Detta utgör enligt regeringens mening ett starkt skäl för att införa en sådan begränsning för myndigheter.

En majoritet av remissinstanserna tillstyrker utredningens förslag eller har inga invändningar mot det. Som Domstolsverket påpekar är ett absolut sökförbud lätt att tillämpa. Flera instanser invänder dock mot bestämmelsens kategoriska utformning och menar att det behövs undantag för att myndigheternas verksamhet ska fungera. *Polismyndigheten* framhåller att det behövs ett undantag för sökningar på känsliga personuppgifter som sker i registervårdande syfte. *Säkerhets- och integritetsskyddsnämnden* anser att förslagets ordalydelse i praktiken kan omöjliggöra en effektiv registervård och tillsyn. *Migrationsverket* och *Specialpedagogiska skolmyndigheten* har synpunkter som rör möjligheterna att ta fram statistik. *Transportstyrelsen* anser att det bör övervägas undantag för myndigheters sökningar i verksamhetssystem där syftet är att följa upp och kvalitetssäkra den egna verksamheten.

Regeringen anser att de synpunkter som lämnats visar att konsekvenserna av ett absolut sökförbud inte är tillräckligt utredda. Detta gäller även i förhållande till offentlighetsprincipen. Det bör också beaktas att den behandling av känsliga personuppgifter som i dag sker med stöd av 8 § PUF eller enligt missbruksregeln i 5 a § PUL inte omfattas av någon sökbegränsning.

Utredningen om 2016 års dataskyddsdirektiv föreslår i sitt delbetänkande Brottsdatalag (SOU 2017:29) en sökbegränsning som i stället utgår från syftet med sökningen. Enligt förslaget till brottsdatalag ska det vara förbjudet att utföra sökningar i syfte att få fram ett personurval grundat på känsliga personuppgifter. En sådan utformning innebär inte större möjligheter att använda känsliga personuppgifter som sökbegrepp vid sådana sökningar som sökförbudet är avsett att hindra, såsom kartläggning av personer på grundval av etnicitet. Detta skulle inte vara tillåtet vare sig enligt Dataskyddsutredningens förslag eller förslaget till brottsdatalag. Däremot skulle en sökbegränsning som utformats i enlighet med förslaget till brottsdatalag inte hindra sökningar som görs för andra ändamål, t.ex. i syfte att utöva tillsyn, för att ta fram verksamhetsstatistik eller för registervård, dvs. då syftet med sökningen inte är att identifiera ett urval av individer.

Regeringen anser, liksom *Skatteverket,* att sökbegränsningarna bör utformas på samma sätt i dataskyddslagen och brottsdatalagen. Mot bakgrund av vad som anförs ovan anser regeringen att en utformning i linje med den som föreslås av Utredningen om 2016 års dataskyddsdirektiv är att föredra även i dataskyddslagen. Det bör således vara förbjudet för myndigheter att utföra sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter. Precis som Dataskyddsutredningen föreslår bör dock detta förbud gälla endast vid sådan behandling av känsliga personuppgifter som utförs med stöd av de särskilda bestäm-

melser som föreslås i detta avsnitt med hänsyn till viktiga allmänna intressen. Detta innebär bl.a. att sökbegränsningen inte gäller vid behandling som sker med stöd av bestämmelser i en registerförfattning. Eftersom dataskyddslagen ska vara subsidiär till avvikande bestämmelser i annan lag eller i förordning kan det även införas undantag från sökbegränsningen på de områden där det behövs, förutsatt att det finns andra lämpliga och särskilda skyddsåtgärder för den registrerade.

Sektorsspecifik reglering

De nu föreslagna bestämmelserna är avsedda att gälla för offentlig verksamhet där sektorsspecifik reglering avseende behandling av känsliga personuppgifter saknas. Det kan finnas anledning att för vissa sektorer närmare precisera och avgränsa möjligheterna att behandla känsliga personuppgifter ytterligare. Ett berättigat behov av att behandla känsliga personuppgifter i större omfattning än vad dessa bestämmelser medger, exempelvis ett behov av att använda sökbegrepp som avslöjar känsliga personuppgifter, kommer också att finnas i vissa verksamheter. Det finns då, precis som i dag, möjlighet att införa sektorsspecifika bestämmelser som är mer tillåtande − exempelvis genom undantag från sökbegränsningen − så länge dessa undantag utformas så att de är förenliga med regeringsformens och dataskyddsförordningens bestämmelser.

Det förtjänar att poängteras att de föreslagna bestämmelserna inte ersätter vare sig artikel 6 eller artikel 9.2 g i dataskyddsförordningen. Den rättsliga grunden för behandlingen måste sökas någon annanstans än i dataskyddslagen. Vidare kan de krav på lämpliga och särskilda åtgärder som ställs i artikel 9.2 g vara uppfyllda även genom andra bestämmelser än de föreslagna. Behandling av känsliga personuppgifter kan alltså ske med stöd av artikel 9.2 g även i andra fall, under förutsättning att lämpliga och särskilda åtgärder fastställts.

Bemyndigande

I 20 § PUL bemyndigas regeringen eller den myndighet som regeringen bestämmer att föreskriva ytterligare undantag om det behövs med hänsyn till ett viktigt allmänt intresse. Bemyndigandet har utnyttjats för att i förordning föreskriva att vissa myndigheter och privata organ får behandla känsliga personuppgifter. Det kommer även i fortsättningen att finnas ett behov av att i förordning kunna tillåta behandling av känsliga personuppgifter med hänsyn till viktiga allmänna intressen för vissa tydligt avgränsade ändamål eller för vissa särskilda verksamheter, utöver de generella bestämmelser som föreslås här. På grund av att dataskyddsförordningen inte innehåller någon motsvarighet till den så kallade missbruksregeln i 5 a § PUL, kommer sannolikt behovet av ytterligare bestämmelser om behandling av känsliga personuppgifter att öka.

Dataskyddslagen bör därför innehålla ett bemyndigande för regeringen att meddela ytterligare föreskrifter om sådan behandling av känsliga personuppgifter som är nödvändig med hänsyn till ett viktigt allmänt intresse. Eftersom regeringen hittills inte har sett anledning att utnyttja möjligheten i 20 § PUL att bemyndiga Datainspektionen att meddela föreskrifter och något behov av sådan vidaredelegation inte har framkommit, föreslås ingen sådan möjlighet.

När nya bestämmelser övervägs med stöd av bemyndigandet måste givetvis en noggrann bedömning göras av om lagform ändå krävs enligt 2 kap. 6 och 20 §§ RF. Det måste också säkerställas att dataskyddsförordningens krav i övrigt är uppfyllda, framför allt när det gäller lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.

10.5 Hälso- och sjukvård och social omsorg

Regeringens förslag: Under förutsättning att kravet på tystnadsplikt enligt EU:s dataskyddsförordning är uppfyllt får känsliga personuppgifter behandlas, om behandlingen är nödvändig för förebyggande hälso- och sjukvård och yrkesmedicin, bedömningen av en arbetstagares arbetskapacitet, medicinska diagnoser, tillhandahållande av hälso- och sjukvård eller behandling, social omsorg eller förvaltning av social omsorg, hälso- och sjukvårdstjänster samt deras system.

Utredningens förslag överensstämmer i sak med regeringens.

Remissinstanserna: Det stora flertalet remissinstanser tillstyrker förslaget eller har inga synpunkter på det. *Socialstyrelsen* och *Diskrimineringsombudsmannen* anser att det är av stor vikt att förutsättningarna för att behandla känsliga personuppgifter är reglerade på ett tydligt sätt. *Hälso- och sjukvårdens ansvarsnämnd* anser att det är angeläget att det finns ett tydligt stöd för att behandla personuppgifter inom tillsyn över hälso- och sjukvård. Vidare anser ansvarsnämnden att det är angeläget att användandet av begreppet arbetstagare inte innebär någon förändring av möjligheten att behandla uppgifter om hälsotillstånd avseende yrkesutövare i reglerade yrken som inte är anställda. *Myndigheten för vård- och omsorgsanalys* anser att det bör förtydligas att begreppet förvaltning av hälso- och sjukvårdstjänster ska tolkas vitt och bl.a. inbegripa behandling som utförs av centrala nationella hälso- och sjukvårdsmyndigheter samt vid tillsyn över hälso- och sjukvård och social omsorg. Myndigheten för vård- och omsorgsanalys anser vidare att begreppet hör samman med medicinska diagnoser bör tydliggöras. *Datainspektionen* anser att det skyndsamt bör utredas huruvida den behandling av personuppgifter som sker i dag inom hälso- och sjukvård och social omsorg är förenlig med artikel 9.2 h och 9.3 i dataskyddsförordningen, eller om det behöver införas en lagstadgad tystnadsplikt för de personuppgiftsbiträden som i dag inte omfattas av en sådan. *Pensionsmyndigheten* anser inte att det är självklart att förordningen ska tolkas så att det finns ett behov av att i dataskyddslagen eller i annan nationell lagstiftning ta in bestämmelser om undantag från förbudet att behandla känsliga personuppgifter. *Dataskydd.net* avstyrker förslaget och anser att artikel 9.2 inte kan kringgås annat än genom lagstiftning som ger behandlingen en rättslig grund, vilket i så fall sker i annan lagstiftning än i dataskyddslagen.

Skälen för regeringens förslag: I dataskyddsförordningen regleras behandling av känsliga personuppgifter på bl.a. hälso- och sjukvårdsområdet i artikel 9.2 h. Bestämmelsen motsvarar artikel 8.3 i dataskyddsdirektivet, som har genomförts i 18 § PUL. Den bestämmelsen anses täcka nästan all behandling av personuppgifter som förekommer inom

hälso- och sjukvårdsområdet. Bland annat omfattas internationellt folkhälsoarbete, kvalitetshöjande behandling av personuppgifter och debitering av avgifter. Behandling av personuppgifter inom hälso- och sjukvården regleras även i t.ex. patientdatalagen (2008:355). Patientdatalagen är dock inte tillämplig hos tillsynsmyndigheterna på hälso- och sjukvårdsområdet.

I dataskyddsförordningen har ytterligare några verksamhetstyper lagts till den uppräkning av verksamheter som anges i direktivets motsvarande artikel, nämligen yrkesmedicin, bedömningen av en arbetstagares arbetskapacitet och social omsorg. Sannolikt omfattar tillägget avseende arbetskapacitet behandling av uppgifter relaterade till sjukskrivning och rehabilitering på arbetet och begreppet social omsorg snarast uppgifter som utförs inom socialtjänsten. Det är dock i avsaknad av praxis svårt att närmare avgränsa innebörden av begreppen.

Vissa andra justeringar, jämfört med direktivets artikeltext, har också gjorts. Bland annat har begreppet administration av hälso- och sjukvård ersatts med förvaltning av hälso- och sjukvårdstjänster och deras system. Av skäl 53 framgår att avsikten är att begreppet förvaltning av hälso- och sjukvårdstjänster ska tolkas vitt och bl.a. inbegripa behandling som utförs av centrala nationella hälsovårdsmyndigheter samt vid tillsyn över hälso- och sjukvård och social omsorg. Detta innebär för svenskt vidkommande att bestämmelsen även omfattar den verksamhet som bedrivs av bl.a. Socialstyrelsen, Inspektionen för vård och omsorg, Folkhälsomyndigheten och Myndigheten för vård- och omsorgsanalys.

För att artikel 9.2 h ska vara tillämplig ställs tre krav som alla måste vara uppfyllda. För det första ska behandlingen vara nödvändig av skäl som hör samman med någon av de angivna verksamheterna, t.ex. medicinska diagnoser eller förvaltning av hälso- och sjukvårdstjänster. De uppräknade verksamhetsområdena torde täcka allt det som omfattas av den befintliga regleringen i 18 § PUL samt social omsorg, liksom tillsyn på hälso- och sjukvårdsområdet och över social omsorg.

För det andra ska den aktuella verksamheten utföras på grundval av unionsrätten eller medlemsstaternas nationella rätt eller enligt avtal med yrkesverksamma på hälsoområdet. Denna förutsättning är enligt regeringens bedömning uppfylld så snart verksamheten bedrivs i enlighet med verksamhetslagstiftningen på de aktuella områdena, t.ex. hälso- och sjukvårdslagen, socialtjänstlagen och andra relevanta författningar. Det är i dessa författningar som den personuppgiftsansvarige finner den rättsliga grunden för att överhuvudtaget få behandla personuppgifter utan den registrerades samtycke.

För att känsliga personuppgifter ska få behandlas i dessa verksamheter krävs dessutom, för det tredje, att förutsättningarna i artikel 9.3 är uppfyllda. Där anges att personuppgifter bara får behandlas av eller under ansvar av en yrkesutövare, eller av en annan person, som omfattas av tystnadsplikt enligt unionsrätten eller medlemsstaternas nationella rätt eller bestämmelser som fastställs av nationella behöriga organ. Sådan tystnadsplikt gäller inom den svenska offentliga sektorn enligt offentlighets- och sekretesslagen. För de privata utförarna finns bestämmelser om tystnadsplikt i bl.a. patientsäkerhetslagen (2010:659) och socialtjänstlagen. *Datainspektionen* anser att det behöver utredas om det därutöver bör införas en lagstadgad tystnadsplikt för hälso- och sjukvårdens

personuppgiftsbiträden. Denna fråga bör övervägas i samband med anpassningen till dataskyddsförordningen av den sektorslagstiftning som finns på hälso- och sjukvårdsområdet och behandlas därför inte i detta lagstiftningsärende.

Regeringen delar i och för sig bl.a. *Pensionsmyndighetens* uppfattning om att det inte behövs någon ytterligare reglering på nationell nivå för att nödvändig behandling av känsliga personuppgifter ska vara tillåten med stöd av artikel 9.2 h. Det är dock, som bl.a. *Socialstyrelsen* betonar, av stor vikt för verksamheten inom de områden som omfattas av bestämmelsen att förutsättningarna för att behandla känsliga personuppgifter framgår tydligt, även för de aktörer som inte omfattas av sektorsspecifika författningar om behandling av känsliga personuppgifter. Det bör därför, i enlighet med utredningens förslag, uttryckligen anges i dataskyddslagen att känsliga personuppgifter får behandlas om behandlingen är nödvändig av skäl som hör samman med förebyggande hälso- och sjukvård och yrkesmedicin, bedömningen av en arbetstagares arbetskapacitet, medicinska diagnoser, tillhandahållande av hälso- och sjukvård eller behandling, social omsorg samt förvaltning av social omsorg, hälso- och sjukvårdstjänster och deras system. Bestämmelsen bör även erinra om att sådan behandling får ske endast under förutsättning att kravet på tystnadsplikt i artikel 9.3 i dataskyddsförordningen är uppfyllt.

Innebörden av de begrepp som används i bestämmelsen bör tolkas och tillämpas på samma sätt som artikel 9.2 h i dataskyddsförordningen. Som nämns ovan framgår det av skäl 53 till dataskyddsförordningen att avsikten är att begreppet förvaltning av hälso- och sjukvårdstjänster ska tolkas vitt och inbegripa bl.a. tillsyn över hälso- och sjukvård. Tolkningen av begreppet arbetstagares arbetskapacitet, som *Hälso- och sjukvårdens ansvarsnämnd* tar upp, påverkar således inte möjligheten till behandling av känsliga personuppgifter inom tillsyn över hälso- och sjukvård.

10.6 Folkhälsa

Regeringens bedömning: Känsliga personuppgifter får enligt EU:s dataskyddsförordning behandlas om behandlingen är nödvändig av skäl av allmänt intresse på folkhälsoområdet, under förutsättning att gällande rätt innehåller lämpliga och specifika åtgärder för att skydda den registrerades rättigheter och friheter, särskilt tystnadsplikt. Det behövs inte någon bestämmelse om detta i dataskyddslagen.

Utredningens bedömning överensstämmer delvis med regeringens. Utredningen bedömer att undantaget måste genomföras i nationell rätt för att vara tillämpligt och att det inte bör införas något sådant undantag i dataskyddslagen.

Remissinstanserna: Endast ett fåtal instanser yttrar sig över utredningens bedömning i denna del. *Folkhälsomyndigheten* invänder mot utredningens bedömning och anser att ett folkhälsoundantag väsentligen skulle underlätta myndighetens arbete och minimera riskerna för att myndigheten inte kommer att kunna genomföra de undersökningar och bearbetningar som behövs för att följa befolkningens hälsa. Även *Forsk-*

ningsrådet för hälsa, arbetsliv och välfärd invänder mot utredningens bedömning och anför att datainsamling inom folkhälsoområdet inte bara gäller det som utredningen definierar som hälso- och sjukvård. *Västra Götalands läns landsting* anser att det vore värdefullt med ett särskilt undantag i dataskyddslagen för behandling av känsliga personuppgifter inom folkhälsoområdet.

Skälen för regeringens bedömning: I förordningens artikel 9.2 i finns ett särskilt undantag från förbudet att behandla känsliga personuppgifter som tar sikte på behandling som är nödvändig av skäl av allmänt intresse på folkhälsoområdet, såsom behovet av att säkerställa ett skydd mot allvarliga gränsöverskridande hot mot hälsan eller säkerställa höga kvalitets- och säkerhetsnormer för vård och läkemedel eller medicintekniska produkter. Bestämmelsen saknar motsvarighet i dataskyddsdirektivet eller personuppgiftslagen.

I skäl 54 anges att termen folkhälsa bör tolkas i enlighet med förordning 1338/2008 om gemenskapsstatistik om folkhälsa och hälsa och säkerhet i arbetet. Den definition som anges där är mycket vid och omfattar alla aspekter som rör hälsosituationen, dvs. allmänhetens hälsotillstånd, inbegripet sjuklighet och funktionshinder, hälsans bestämningsfaktorer, hälso- och sjukvårdsbehov, resurser inom hälso- och sjukvården, tillhandahållande av och allmän tillgång till hälso- och sjukvård, utgifter för och finansiering av hälso- och sjukvården samt dödsorsaker.

För att behandling av känsliga personuppgifter ska vara tillåten enligt artikel 9.2 i krävs för det första att behandlingen är nödvändig av skäl av allmänt intresse på folkhälsoområdet, på grundval av unionsrätten eller medlemsstatens nationella rätt. Detta innebär enligt regeringens bedömning att den personuppgiftsansvarige ska ha stöd i rättsordningen för att utföra en uppgift på folkhälsoområdet. Detta rättsliga stöd ska enligt artikel 9.2 i innehålla lämpliga och specifika åtgärder för att skydda den registrerades rättigheter och friheter, särskilt tystnadsplikt. Tröskeln för att den personuppgiftsansvarige ska få behandla känsliga personuppgifter som ett led i att utföra sin uppgift på folkhälsoområdet är således högre än den som gäller för behandling av andra personuppgifter i samma verksamhet.

Utredningen bedömer att undantaget i artikel 9.2 i måste genomföras i nationell rätt för att vara tillämpligt. Regeringen anser emellertid att undantaget är direkt tillämpligt och att känsliga personuppgifter får behandlas med stöd av artikel 9.2 i, om kravet på lämpliga och specifika åtgärder för att skydda den registrerades rättigheter och friheter är uppfyllt. Regeringen gör således till skillnad från utredningen bedömningen att undantaget i sig inte måste genomföras i svensk rätt för att vara tillämpligt.

Folkhälsoarbete anses i Sverige vara tvärsektoriellt och involverar såväl statliga som kommunala myndigheter. I den mån känsliga personuppgifter behöver behandlas som ett led i detta folkhälsoarbete bör dessa vara sekretessreglerade i verksamheten. Till exempel regleras sekretess hos statistikmyndigheterna i 24 kap. 8 § OSL och sekretess inom hälso- och sjukvården liksom vid åtgärder mot smittsamma sjukdomar i 25 kap. OSL. Vidare gäller viss sekretess enligt offentlighets- och sekretesslagen och offentlighets- och sekretessförordningen (2009:641) hos bl.a. Folkhälsomyndigheten, Tandvårds- och läkemedelsförmånsverket och Forsk-

ningsrådet för hälsa, arbetsliv och välfärd samt vid tillsyn enligt bl.a. livsmedelslagen (2006:804) och läkemedelslagen (2015:315). Dessutom gäller under vissa förutsättningar sekretess enligt 21 kap. 1 § OSL för uppgift som rör en enskilds hälsa eller sexualliv, oavsett var uppgiften förekommer.

Enligt regeringens bedömning är förutsättningarna för att behandling ska få ske enligt artikel 9.2 i uppfyllda om de känsliga personuppgifterna är sekretessreglerade i verksamheten. Om sekretessreglering saknas kan det däremot inte tas för givet att dataskyddsförordningens krav på lämpliga och specifika åtgärder för att skydda den registrerades rättigheter och friheter är uppfyllda.

Det hade i och för sig varit möjligt att, på motsvarande sätt som föreslås avseende artikel 9.2 h, införa en motsvarighet till förordningens bestämmelse i dataskyddslagen. Utredningen lämnar dock inte något sådant förslag. Enligt regeringens bedömning, som skiljer sig från utredningens, behövs det heller inte någon ytterligare reglering på generell nivå för att behandling av känsliga personuppgifter ska kunna ske med stöd av artikel 9.2 i. Om det på något specifikt område eller för någon enskild myndighet bedöms att befintliga skyddsåtgärder är otillräckliga, bör den frågan övervägas i ett annat sammanhang.

11 Personuppgifter som rör lagöverträdelser

Regeringens förslag: Personuppgifter som rör lagöverträdelser får behandlas av myndigheter.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter som tillåter andra än myndigheter att behandla sådana uppgifter. Den myndighet som regeringen bestämmer får i enskilda fall besluta om att tillåta sådan behandling. Ett beslut får förenas med villkor.

Utredningens förslag överensstämmer i huvudsak med regeringens. I utredningens förslag anges inte att beslut får förenas med villkor. Vidare har utredningens förslag en annan språklig utformning.

Remissinstanserna: Det stora flertalet remissinstanser tillstyrker förslaget eller har inga synpunkter på det. *Datainspektionen* delar utredningens uppfattning om att artikel 10 i dataskyddsförordningen kan tolkas som att inspektionen i viss mån kan vara något mindre restriktiv än tidigare med att tillåta andra än myndigheter att behandla uppgifter om lagöverträdelser, men efterlyser mer vägledning för när det kan vara motiverat. *Sveriges akademikers centralorganisation* och *Sveriges Ingenjörer* anser att beslut som tillåter behandling av personuppgifter i enskilda fall bör meddelas mycket restriktivt. *Riksidrottsförbundet* påtalar idrottsrörelsens behov av att behandla personuppgifter som rör lagöverträdelser, bl.a. för att motverka dopning och matchfixning. Flera remissinstanser som företräder näringslivet, bl.a. *Svensk Handel*, *Teknikföretagen* och *Svenskt Näringsliv*, anser att det ska vara tillåtet att behandla personuppgifter som rör lagöverträdelser när detta krävs enligt

utländska regelverk, bl.a. vid handel med tredjeland. Några av dessa, samt *Svensk Försäkring* och *Sveriges advokatsamfund*, ifrågasätter utredningens bedömning av i vilken mån misstanke om brott innefattas i begreppet överträdelser. *Dataskydd.net* anser att bestämmelsen bör ange att de myndigheter som regeringen bestämmer får behandla personuppgifter som rör lagöverträdelser och att dessa myndigheter får medge andra än myndigheter att behandla sådana uppgifter i vissa specifika fall.

Skälen för regeringens förslag

Fällande domar i brottmål samt överträdelser

Uppgifter som rör lagöverträdelser tillhör inte de särskilda kategorier av personuppgifter som omfattas av förbudet mot behandling i artikel 9 i dataskyddsförordningen, men anses ändå vara en kategori personuppgifter som förtjänar särskilt skydd. Enligt artikel 10 får behandling av personuppgifter som rör fällande domar i brottmål och överträdelser eller därmed sammanhängande säkerhetsåtgärder utföras endast under kontroll av myndighet eller då behandling är tillåten enligt unionsrätten eller medlemsstaternas nationella rätt, där lämpliga skyddsåtgärder för de registrerades rättigheter och friheter fastställs. Ett fullständigt register över fällande domar i brottmål får endast föras under kontroll av en myndighet.

Artikel 10 i dataskyddsförordningen motsvarar artikel 8.5 i dataskyddsdirektivet, som har genomförts i svensk rätt genom 21 § PUL. Tillämpningsområdet för förordningens bestämmelse är dock något mer begränsad. Vid en jämförelse med andra språkversioner tycks begreppet överträdelser i artikel 10 inte avse vilka överträdelser som helst, utan endast sådana som utgör en brottslig gärning. Begreppet överträdelser kan därför anses som likvärdigt med det snävare uttryck som används i personuppgiftslagen, dvs. lagöverträdelser som innefattar brott. Justitiedepartementet har mot denna bakgrund lämnat in en begäran om korrigering av den svenska språkversionen av dataskyddsförordningen (Ju2016/00482/L6).

En betydande skillnad jämfört med direktivet är att artikel 10 i förordningen inte ger medlemsstaterna någon möjlighet att på denna grund begränsa behandlingen av personuppgifter om administrativa sanktioner och avgöranden i tvistemål. Uppgifter om administrativa frihetsberövanden omfattas således inte av någon särskild reglering enligt dataskyddsförordningen, om de inte utgör känsliga personuppgifter enligt artikel 9.1, exempelvis om de också avslöjar uppgifter om etniskt ursprung eller psykisk ohälsa.

Begreppet säkerhetsåtgärder bedömdes vid genomförandet av dataskyddsdirektivet som likvärdigt med straffprocessuella tvångsmedel. Denna bedömning framstår som rimlig även i förhållande till begreppet därmed sammanhängande säkerhetsåtgärder, som används i dataskyddsförordningen.

Särskilt om misstanke om brott

Frågan om i vilken utsträckning brottsmisstankar omfattas av begreppet lagöverträdelser som innefattar brott har varit föremål för diskussion.

Datalagskommittén menade att en uppgift om att någon har eller kan ha begått stöld otvivelaktigt utgör en uppgift om lagöverträdelse, även om det inte finns någon dom beträffande brottet. Uppgifter om faktiska iakttagelser om en persons handlande kunde dock enligt Datalagskommittén inte rimligen anses som uppgifter om lagöverträdelser i alla de fall handlandet kan innebära en lagöverträdelse (SOU 1997:39 s. 380). Högsta förvaltningsdomstolen har i det s.k. TankStopp-målet (HFD 2016 ref. 8) uttalat att registrering av uppgifter om fordon som förekommit i samband med obetalda tankningar ska anses innefatta en behandling av personuppgifter om lagöverträdelser som innefattar brott i den mening som avses i personuppgiftslagen. Utredningen har mot denna bakgrund, i avsaknad av klargörande EU-rättslig praxis, bedömt att misstankar om brott bör omfattas av artikel 10 i dataskyddsförordningen i samma utsträckning som de gör enligt personuppgiftslagen. Flera remissinstanser invänder mot denna bedömning och anser att den saknar stöd i dataskyddsförordningen. *Svensk Handel* konstaterar bl.a. att kamerabevakning skulle bli omöjlig och helt utan verkan för det fall det alltid skulle vara förbjudet för andra än myndigheter att behandla personuppgifter som innefattar misstanke om brott. Svensk Handel menar att det inte kan vara avsikten med vare sig dataskyddsförordningen, dataskyddslagen eller kamerabevakningslagen.

Ett av de huvudsakliga syftena med dataskyddsförordningen är att åstadkomma en ytterligare harmonisering av dataskyddsregleringen för att undanröja hindren för det fria flödet av personuppgifter inom EU (se t.ex. skäl 9 och 13). Det är därför angeläget att artikel 10 inte tolkas på ett mer extensivt sätt i Sverige än i andra medlemsstater. Som konstateras ovan har artikel 10 en annan utformning än motsvarande reglering i dataskyddsdirektivet och personuppgiftslagen. Det är därför, som bl.a. Svensk Handel är inne på, inte säkert att praxis enligt personuppgiftslagen kring vilka uppgifter som omfattas av regleringen om personuppgifter som rör lagöverträdelser fortfarande är aktuell.

När det gäller kameraövervakning kan konstateras att Utredningen om kameraövervakning – Brottsbekämpning och integritetsskydd (Ju 2015:14) anser att artikel 10 måste tolkas så att den inte tar sikte på sådana möjliga lagöverträdelser som kan fångas på bild vid kameraövervakning (SOU 2017:55 s. 121). Regeringen instämmer i den bedömningen.

Behandling under kontroll av en myndighet

Den del av artikel 10 som rör behandling av uppgifter under kontroll av myndighet är direkt tillämplig. Det är emellertid inte tydligt vad begreppet under kontroll av myndighet innebär för svenskt vidkommande. Begreppet skulle kunna tolkas som att behandlingen ska ske av ett organ som anförtrotts uppgifter som ankommer på den offentliga sektorn. Till skillnad från *dataskydd.net* bedömer regeringen att bestämmelsen i artikel 10 i vart fall bör innebära att det är tillåtet att behandla uppgifter som rör lagöverträdelser om den personuppgiftsansvarige är en myndighet. Det är angeläget att tydliggöra detta, eftersom det innebär att myndigheter inte behöver uttryckligt stöd i föreskrifter eller särskilda beslut för att få behandla sådana uppgifter. Förordningens skäl 8 ger

uttryck för att medlemsstaterna får införliva delar av förordningen i nationell rätt, om det krävs för att göra de nationella bestämmelserna begripliga för de personer de tillämpas på. Det finns således ett visst utrymme att förtydliga innebörden av artikel 10 i svensk rätt. Som utredningen föreslår bör det därför uttryckligen framgå av dataskyddslagen att personuppgifter som rör lagöverträdelser får behandlas av myndigheter.

Behandling som är tillåten enligt nationell rätt

Huvudregeln i 21 § PUL innebär att det är förbjudet för andra än myndigheter att behandla personuppgifter som rör lagöverträdelser. Undantag från detta förbud kan dock meddelas genom föreskrifter eller beslut i enskilda fall. Något sådant principiellt förbud mot behandling av denna typ av personuppgifter finns inte i dataskyddsförordningen. Enligt artikel 10 i dataskyddsförordningen får behandling ske utan kontroll av myndighet då behandlingen är tillåten enligt unionsrätten eller medlemsstaternas nationella rätt, där lämpliga skyddsåtgärder fastställs. Regleringen i artikel 10 syftar således till att säkerställa att det i unionsrätten eller den nationella rätten finns lämpliga skyddsåtgärder för de registrerades rättigheter och friheter, när behandling utförs av andra än myndigheter.

Enligt regeringens mening är det inte lämpligt att i dataskyddslagen ange vilka skyddsåtgärder som bör finnas vid behandling av uppgifter om lagöverträdelser. I stället bör detta övervägas i särskild ordning där behovet kan analyseras särskilt från fall till fall. Regeringen föreslår därför i likhet med utredningen att regeringen eller den myndighet regeringen bestämmer ska ges befogenhet att meddela föreskrifter som tillåter andra än myndigheter att behandla personuppgifter som rör lagöverträdelser. Regeringen har för avsikt att, som utredningen föreslår, vidaredelegera denna normgivningskompetens till tillsynsmyndigheten.

Eftersom dataskyddslagen föreslås vara subsidiär i förhållande till andra lagar och förordningar, kommer det även i fortsättningen att finnas utrymme för särreglering som tillåter behandling av personuppgifter som rör lagöverträdelser, t.ex. av sådant slag som i dag finns i lagen (2015:51) om register över tillträdesförbud vid idrottsarrangemang. Det bör dock noteras att det inte krävs en uttrycklig undantagsreglering för att behandling av uppgifter som rör lagöverträdelser ska vara tillåten. Således är det tillåtet att behandla sådana personuppgifter om det krävs för att t.ex. uppfylla en editionsplikt eller ett informationsföreläggande som meddelats av domstol med stöd av lag.

Som utredningen föreslår bör den myndighet som regeringen bestämmer även ges befogenhet att i enskilda fall besluta att andra än myndigheter får behandla uppgifter om lagöverträdelser. Regeringen har för avsikt att peka ut tillsynsmyndigheten som ansvarig för den uppgiften. Enligt regeringens bedömning kan kravet på lämpliga skyddsåtgärder i artikel 10 i princip vara uppfyllt genom den tillståndsprövning som föregår sådana beslut i enskilda fall. Besluten kan dock vid behov även förenas med villkor såsom återkallelseförbehåll, tidsbegränsningar eller krav på återrapportering samt krav på att den personuppgiftsansvarige

ska vidta vissa åtgärder till skydd för de registrerades rättigheter och friheter.

Utöver kravet på lämpliga skyddsåtgärder ställer dataskyddsförordningen inte upp några begränsningar i fråga om medlemsstaternas möjlighet att i sin nationella rätt tillåta andra än myndigheter att behandla personuppgifter som rör lagöverträdelser. Detta innebär att utrymmet för att tillåta sådan behandling genom föreskrifter och beslut i enskilda fall blir större än enligt personuppgiftslagen, eftersom denna utgår från att behandlingen är förbjuden. Tillsynsmyndighetens utrymme att avslå en begäran om tillstånd torde i princip vara begränsat till de fall där behandlingen skulle vara oförenlig med dataskyddsförordningen i övrigt, i synnerhet principerna i artikel 5 och kravet på rättslig grund i artikel 6. I annat fall bör tillstånd beviljas, men vid behov förenas med krav på lämpliga skyddsåtgärder för de registrerades rättigheter och friheter.

Flera remissinstanser, bl.a. *Svensk Handel*, *Teknikföretagen* och *Svenskt Näringsliv*, påtalar att svenska exportföretag måste behandla vissa uppgifter som rör lagöverträdelser på grund av att utländska regelverk ställer krav på kontroll mot vissa sanktions- eller spärrlistor. De ger uttryck för en oro för att Sverige ska inta en mer restriktiv hållning än vad dataskyddsförordningen kräver, vilket skulle försämra möjligheterna för svenska företag att konkurrera på en internationell marknad. Det är regeringens uppfattning att svenska företag inte ska ges sämre möjligheter att behandla uppgifter som rör lagöverträdelser än företag i andra länder. Regeringen kan också konstatera att det typiskt sett bör vara möjligt för svenska exportföretag att få tillstånd att behandla sådana uppgifter i den mån detta krävs för sådan kontroll mot sanktions- och spärrlistor som är nödvändig för export till vissa länder. Detta bör i vart fall gälla om dessa listor är fastställda i demokratisk ordning och allmänt tillgängliga.

Några remissinstanser pekar på att systemet med särskilda beslut i enskilda fall är betungande för både tillsynsmyndigheten och företagen, varför föreskrifter som tillåter nödvändig behandling är att föredra. Med anledning av denna synpunkt vill regeringen understryka att det, t.ex. i fråga om vissa viktigare spärr- och sanktionslistor, kan finnas anledning för tillsynsmyndigheten att använda möjligheten att meddela föreskrifter. Detta kan minska den administrativa bördan både för företagen och för tillsynsmyndigheten själv.

I detta sammanhang bör även nämnas att behovet av särskilda föreskrifter eller beslut i enskilda fall också torde öka som en följd av att den så kallade missbruksregeln i 5 a § PUL saknar motsvarighet i dataskyddsförordningen.

12 Personnummer och samordningsnummer

Regeringens förslag: Personnummer och samordningsnummer får behandlas utan samtycke endast när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl.

Regeringen får meddela ytterligare föreskrifter om behandling av personnummer och samordningsnummer.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Det stora flertalet tillstyrker förslaget eller har inga synpunkter på det. *Kammarrätten i Göteborg* konstaterar att 22 § PUL inte behöver tillämpas vid sådan behandling av personuppgifter i ostrukturerat material som avses i 5 a § PUL och efterfrågar överväganden om det är ett undantag som fortsatt bör gälla avseende personnummer och samordningsnummer. *Dataskydd.net* anser att uppgifter om personnummer eller samordningsnummer ska få behandlas utan samtycke endast när det är klart motiverat med hänsyn till ändamålet med behandlingen samt att tillsynsmyndigheten bör bemyndigas att meddela föreskrifter.

Skälen för regeringens förslag: Personnummer och samordningsnummer utgör inte känsliga personuppgifter i dataskyddsförordningens mening, men har ändå getts en särställning genom att medlemsstaterna getts möjlighet att införa särskilda villkor för behandlingen (artikel 87). Villkoren ska i sådana fall säkerställa att identifikationsuppgifterna bara får användas med iakttagande av lämpliga skyddsåtgärder för de registrerades fri- och rättigheter. Något uttryckligt krav på skyddsåtgärder finns inte enligt dataskyddsdirektivet. Förordningens bestämmelse överensstämmer i övrigt med artikel 8.7 i dataskyddsdirektivet, som har genomförts i 22 § PUL. De villkor som uppställs i 22 § PUL innebär att uppgifter om personnummer och samordningsnummer får behandlas utan samtycke bara när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl.

Regleringen i 22 § PUL ger uttryck för att behandlingen av personnummer och samordningsnummer bör vara restriktiv och föregås av en intresseavvägning mellan behovet av behandlingen och de integritetsrisker som den innebär. Bestämmelsen ligger väl i linje också med förordningens intentioner och är enligt regeringens mening flexibel och väl avpassad för att förhindra omotiverad behandling av personnummer och samordningsnummer. Regeringen anser därför, till skillnad från *dataskydd.net*, att en bestämmelse som i sin helhet motsvarar 22 § PUL bör införas i dataskyddslagen.

I 50 § c PUL anges att regeringen eller den myndighet som regeringen bestämmer, dvs. Datainspektionen enligt 16 § PUF, får meddela närmare föreskrifter om i vilka fall användning av personnummer är tillåten. Några sådana föreskrifter har inte meddelats av Datainspektionen. Det är däremot relativt vanligt med sektorsspecifika förordningsbestämmelser om behandling av personnummer och samordningsnummer. Det kommer även fortsättningsvis att finnas behov för regeringen att meddela sådana

föreskrifter. Det saknas dock skäl för regeringen att i detta lagstiftningsärende ta ställning till om det finns ett sådant behov när det gäller den typ av ostrukturerad behandling som *Kammarrätten i Göteborg* nämner.

Som utredningen föreslår bör det därför införas ett bemyndigande i dataskyddslagen som avser föreskrifter om personnummer och samordningsnummer. Eftersom Datainspektionen hittills inte har sett anledning att utnyttja möjligheten enligt 16 § PUF att meddela föreskrifter och något behov av sådan vidaredelegation inte har framkommit, föreslås däremot ingen sådan möjlighet.

En bestämmelse om behandling av personnummer och samordningsnummer kan, oavsett om den tas in direkt i sektorsspecifik lag eller i förordning med stöd av bemyndigandet, tillåta behandling i andra fall än de som tillåts enligt den föreslagna bestämmelsen i dataskyddslagen. En avvikande bestämmelse måste dock leva upp till förordningens krav på lämpliga skyddsåtgärder för de registrerades fri- och rättigheter.

Sammanfattningsvis föreslår alltså regeringen att personnummer och samordningsnummer ska få behandlas utan samtycke endast när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl. Vidare föreslås att regeringen ska få meddela ytterligare föreskrifter om behandling av personnummer och samordningsnummer.

13 Begränsningar av vissa rättigheter och skyldigheter i dataskyddsförordningen

Regeringens förslag: Bestämmelserna i EU:s dataskyddsförordning om information och tillgång till personuppgifter gäller inte uppgifter som den personuppgiftsansvarige inte får lämna ut till den registrerade enligt lag eller annan författning eller enligt beslut som meddelats med stöd av författning. Om den personuppgiftsansvarige inte är en myndighet gäller undantaget för uppgifter som hos en myndighet skulle ha varit sekretessbelagda enligt offentlighets- och sekretesslagen.

Bestämmelsen i EU:s dataskyddsförordning om den registrerades rätt till tillgång gäller inte personuppgifter i löpande text som utgör utkast eller minnesanteckning eller liknande. Undantaget gäller dock inte om uppgifterna har lämnats ut till tredje part, om uppgifterna behandlas enbart för arkivändamål av allmänt intresse eller för statistiska ändamål eller om de har behandlats under längre tid än ett år i löpande text som inte har fått sin slutliga utformning.

Regeringen får meddela ytterligare föreskrifter om begränsningar enligt EU:s dataskyddsförordning.

Regeringens bedömning: Rätten att göra invändningar mot myndigheters behandling av personuppgifter bör inte begränsas genom ett undantag i dataskyddslagen. Sådana begränsningar bör i stället vid behov övervägas på sektorspecifik nivå.

Utredningens förslag och bedömning överensstämmer i huvudsak med regeringens. I utredningens förslag till bemyndigande nämns inte artikel 89.2–3 i dataskyddsförordningen i författningstexten.

Remissinstanserna: Det stora flertalet remissinstanser tillstyrker utredningens förslag och instämmer i dess bedömning eller har inga synpunkter på dem. Enligt *Kronofogdemyndigheten* utgör de föreslagna bestämmelserna om undantag från informationsskyldigheten nödvändiga anpassningar till tryckfrihetsförordningens och offentlighets- och sekretesslagens bestämmelser. *Pensionsmyndigheten* anser att det bör förtydligas på vilken grund i artikel 23.1 som den registrerades rättigheter begränsas. *Riksrevisionen* bedömer att undantagen i artikel 14.5 b och c är tillämpliga i granskningsverksamheten, men anser att det vore önskvärt med ett förtydligande, t.ex. en bestämmelse som särskilt reglerar möjligheten för myndigheter som bedriver granskning och tillsyn att göra undantag från informationsskyldigheten. *Svenska bankföreningen* anser att den registrerades rätt till dataportabilitet inte ska gälla i fråga om uppgifter som hos en myndighet skulle ha varit sekretessbelagda enligt offentlighets- och sekretesslagen. *Förvaltningsrätten i Stockholm* kan se problem med att effektuera en begäran om information som ska lämnas enligt artikel 14, dvs. information om personuppgifter som inte har erhållits från den registrerade, och som behandlas i löpande text. *Länsstyrelsen i Kronobergs län* ifrågasätter utredningens förslag om att utkast till allmänna handlingar ska kunna lämnas ut om de varit utkast i mer än ett år. Även *Svensk Försäkring* anser att tidsgränsen på ett år ska förlängas. *Srf konsulternas förbund* anser att vad som kan anses vara minnesanteckningar och när en text är färdigställd kan bli svårdefinierat. *Kammarrätten i Göteborg* håller med om att den registrerades rätt att göra invändningar inte bör begränsas, men efterfrågar exempel på vad som kan utgöra tvingande berättigade skäl som kan anses väga tyngre än den registrerades intressen. *Försvarsmakten* anser däremot att undantag ska meddelas avseende den registrerades rätt att göra invändningar. *Centrala studiestödsnämnden* har förståelse för att utredningen inte bedömer det lämpligt att föreslå en generell inskränkning av rätten att invända, men påpekar att hanteringen mycket väl kan bli administrativt resurskrävande. *Post- och telestyrelsen* och *Konkurrensverket* noterar att utredningen inte uttryckligen berör frågan om invändningsrätt vid myndighetsutövning. *Malmö kommun* anser att det noga bör övervägas om det finns behov att införa ett generellt undantag från rätten att göra invändningar i dataskyddslagen särskilt när det gäller myndigheter, men förstår varför utredningen anser att sådana undantag bör övervägas på sektorspecifik nivå. *Svensk Försäkring* anser att bemyndigandet att meddela ytterligare begränsningar ska kunna vidaredelegeras till Datainspektionen, då ett sådant förfarande skulle göra regleringen mer flexibel. *Dataskydd.net* tillstyrker undantag från artikel 15 på grund av sekretess, men avstyrker förslagen i övrigt. Dataskydd.net anför att undantag för löptext saknar stöd i dataskyddsförordningen, som är teknikneutral och inte ska avgränsas till sökbara register.

Skälen för regeringens förslag

Regleringen i förordningen

I dataskyddsförordningen har den registrerades rättigheter förstärkts i syfte att ge den registrerade ökad kontroll över sina personuppgifter.

Den information som ska tillhandahållas den registrerade har preciserats och utvidgats och det anges uttryckligen att den personuppgiftsansvarige ska tillhandahålla informationen i en begriplig och lättillgänglig form. Den personuppgiftsansvariges skyldighet att självmant tillhandahålla den registrerade information om behandlingen av personuppgifter anges i artiklarna 13 och 14. Den registrerade har vidare enligt artikel 15 rätt att på begäran få tillgång till de personuppgifter som behandlas och viss information.

Enligt artikel 16 har den registrerade rätt att på begäran få felaktiga personuppgifter rättade. Förutsättningarna för att den registrerade ska få sina personuppgifter raderade anges i artikel 17 (rätten att bli bortglömd). Vidare anges i artikel 18 att den registrerade under vissa omständigheter har rätt att kräva att behandlingen begränsas.

Förordningen innehåller i artikel 20 en bestämmelse som ger den registrerade rätt att få åtkomst till sina personuppgifter i syfte att föra över dem till en annan leverantör av elektroniska tjänster, s.k. dataportabilitet, om behandlingen grundar sig på den registrerades samtycke eller avtal med denne.

Enligt artikel 21 har den registrerade rätt att göra invändningar mot behandling av personuppgifter som grundar sig på artikel 6.1 e eller f, dvs. som sker för att utföra en uppgift av allmänt intresse, i myndighetsutövning eller efter en intresseavvägning. Slutligen har den registrerade enligt huvudregeln i artikel 22 rätt att inte bli föremål för ett automatiserat individuellt beslutsfattande, inbegripet profilering.

I artikel 23.1 i dataskyddsförordningen anges att såväl unionsrätten som en medlemsstats nationella rätt får begränsa tillämpningsområdet för vissa skyldigheter och rättigheter som föreskrivs i förordningen, om en sådan begränsning sker med respekt för andemeningen i de grundläggande rättigheterna och friheterna och utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle i syfte att säkerställa vissa särskilt angivna mål. Bestämmelsen motsvarar delvis artikel 13.1 i dataskyddsdirektivet. Möjlighet att begränsa vissa av de registrerades rättigheter ges även i artikel 89.2 i förordningen, i fråga om behandling av personuppgifter för vetenskapliga eller historiska forskningsändamål eller statistiska ändamål. Enligt artikel 89.3 får vissa rättigheter också begränsas vid behandling av personuppgifter för arkivändamål av allmänt intresse.

Rätten att göra invändningar

I artikel 21 i dataskyddsförordningen föreskrivs att den registrerade i vissa fall ska ha rätt att invända mot behandling av personuppgifter. Bestämmelsen är direkt tillämplig. En motsvarande rättighet föreskrivs även i dataskyddsdirektivet, men är genomförd i personuppgiftslagen endast såvitt avser direkt marknadsföring (11 § PUL). Dataskyddsförordningen innebär därmed att rätten att göra invändningar utvidgas jämfört med vad som följer av gällande svensk rätt. Rätten att göra invändningar

enligt artikel 21.1 i dataskyddsförordningen avser behandling av personuppgifter som grundar sig på artikel 6.1 e eller f, dvs. som ett led i myndighetsutövning, för att utföra en uppgift av allmänt intresse eller efter en intresseavvägning. Rättigheten gäller alltså inte vid behandling av personuppgifter som exempelvis är nödvändig för att den personuppgiftsansvarige ska kunna uppfylla en rättslig förpliktelse (artikel 6.1 c), t.ex. när en myndighet genom författning har ålagts att föra ett register. Följden av att en invändning görs enligt artikel 21.1 är att den personuppgiftsansvarige inte längre får behandla personuppgifterna, såvida inte denne kan påvisa tvingande berättigade skäl för behandlingen som väger tyngre än den registrerades intressen, rättigheter och friheter eller om det sker för fastställande, utövande eller försvar av rättsliga anspråk.

Enligt gällande svensk rätt har den registrerade inte någon generell rätt att göra invändningar mot den behandling av personuppgifter som sker hos myndigheter. Det finns mot den bakgrunden skäl att särskilt överväga om dataskyddsförordningens rätt att göra invändningar bör inskränkas, med stöd av artikel 23, när det gäller sådan behandling som sker med stöd av artikel 6.1 e, dvs. som ett led i myndighetsutövning eller för att utföra en uppgift av allmänt intresse.

Som utredningen anför fyller rätten att göra invändningar en viktig funktion ur rättssäkerhetssynpunkt, i synnerhet i de fall då de närmare villkoren för behandlingen inte har reglerats i en sektorsspecifik författning. Regeringen anser därför i likhet med utredningen, till skillnad från bl.a. *Försvarsmakten*, att rätten att göra invändningar mot myndigheters behandling av personuppgifter inte bör inskränkas på ett generellt plan genom ett undantag i dataskyddslagen. Sådana undantag bör i stället övervägas på sektorspecifik nivå.

Med anledning av *Kammarrätten i Göteborgs* synpunkter bör framhållas att en myndighet som kan visa att behandling av personuppgifter är nödvändig som ett led i myndighetsutövning eller för att utföra en uppgift av allmänt intresse typiskt sett bör anses ha påvisat sådana tvingande berättigade skäl som kan anses väga tyngre än den registrerades intressen.

Sekretess och tystnadsplikt ska gå före informationsplikten och rätten till tillgång

Om personuppgifter som rör en registrerad person samlas in från den registrerade, ska den personuppgiftsansvarige enligt artikel 13 självmant lämna viss information till den registrerade, bl.a. om ändamålen med och den rättsliga grunden för behandlingen. Den personuppgiftsansvariges skyldighet att förse den registrerade med sådan information i de fall personuppgifterna inte har erhållits från den registrerade anges i artikel 14.

I artikel 14.5 föreskrivs flera undantag från bestämmelserna om den registrerades rätt till information när personuppgifter inte har erhållits från den registrerade. Enligt artikel 14.5 b ska dessa bestämmelser inte tillämpas i den mån tillhandahållandet av sådan information visar sig vara omöjligt eller skulle medföra en oproportionell ansträngning. Enligt artikel 14.5 c ska bestämmelserna inte heller tillämpas om erhållande

eller utlämnande av uppgifter uttryckligen föreskrivs genom unionsrätten eller genom en medlemsstats nationella rätt som den registrerade omfattas av och som fastställer lämpliga åtgärder för att skydda den registrerades berättigade intressen. Detta innebär bl.a. att en tillsynsmyndighet som regel inte behöver informera den registrerade om behandlingen av sådana personuppgifter som myndigheten erhållit som en följd av en reglerad uppgiftsskyldighet. Undantagen i artikel 14.5 är direkt tillämpliga och behöver inte, som *Riksrevisionen* förordar, upprepas eller förtydligas i dataskyddslagen.

I 27 § PUL anges att bestämmelserna i 23–26 §§ om den registrerades rätt till information inte gäller i den utsträckning det är särskilt föreskrivet i lag eller annan författning eller annars framgår av beslut som har meddelats med stöd av författning att uppgifter inte får lämnas ut till den registrerade. En personuppgiftsansvarig som inte är en myndighet får därvid i motsvarande fall som avses i offentlighets- och sekretesslagen vägra att lämna ut uppgifter till den registrerade. Frågan är om motsvarande undantag bör tas in i dataskyddslagen.

I artikel 14.5 d i dataskyddsförordningen anges att den personuppgiftsansvariges informationsplikt när personuppgifter inte har erhållits från den registrerade inte ska tillämpas om personuppgifterna måste förbli konfidentiella till följd av tystnadsplikt enligt unionsrätt eller nationell rätt, inbegripet lagstadgade sekretessförpliktelser. I artikel 15.4 anges endast att den registrerades rätt till tillgång inte ska inverka menligt på andras friheter och rättigheter.

Det befintliga undantaget i 27 § PUL är vidare än de direkt tillämpliga undantagen i artiklarna 14.1 d och 15.4. Något tydligt undantag från rätten till tillgång enligt artikel 15 finns inte i dataskyddsförordningen i fråga om uppgifter som omfattas av sekretess eller tystnadsplikt. Vidare finns det situationer då även en privaträttslig aktör, som inte omfattas av författningsreglerad sekretess eller tystnadsplikt, har berättigad anledning att hemlighålla uppgifter i förhållande till den registrerade. Det kan t.ex. röra sig om information som samlats in inför en domstolsprocess, om det kan antas att ett utlämnande av informationen skulle försämra den personuppgiftsansvariges ställning som part i rättegången. Regeringen anser därför i likhet med utredningen att det finns ett behov av ett undantag motsvarande det som i dag finns i 27 § PUL.

Pensionsmyndigheten efterfrågar förtydliganden av på vilken grund i artikel 23.1 som den registrerades rättigheter begränsas. När det gäller den offentliga sektorn kan konstateras att reglerna om sekretess i offentlighets- och sekretesslagen utgör begränsningar av rätten att ta del av allmänna handlingar. Denna rätt får enligt 2 kap. 2 § TF begränsas endast om det är påkallat med hänsyn till vissa särskilt angivna ändamål, t.ex. rikets säkerhet, intresset att förebygga eller beivra brott eller skyddet för enskildas personliga eller ekonomiska förhållanden. De godtagbara ändamål för sekretess som anges i tryckfrihetsförordningen utgör också godtagbara ändamål för begränsningar av den registrerades rättigheter enligt artikel 23.1 i dataskyddsförordningen. När det gäller andra än myndigheter ger den sistnämnda bestämmelsen också medlemsstaterna utrymme att göra sådana undantag i syfte att säkerställa skydd av andras fri- och rättigheter och verkställighet av civilrättsliga krav. Det är således tillåtet att föreskriva undantag från de registrerades rättigheter med

hänsyn till privaträttsliga aktörers berättigade behov av att hemlighålla uppgifter. Enligt regeringens bedömning respekterar ett undantag som motsvarar 27 § PUL andemeningen i de grundläggande rättigheterna och friheterna och utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle.

Det bör därför, som utredningen föreslår, införas ett undantag från informationsplikten som i sak motsvarar 27 § PUL. Praxis rörande 27 § PUL bör kunna vara vägledande även vid tillämpningen av den nya bestämmelsen.

Svenska bankföreningen anser att ett motsvarande undantag bör införas även avseende den registrerades rätt till dataportabilitet, i fråga om uppgifter som hos en myndighet skulle ha varit sekretessbelagda enligt offentlighets- och sekretesslagen. Denna fråga behandlas inte av utredningen. Det har, enligt regeringens bedömning, inte framkommit skäl att införa ett sådant generellt undantag i dataskyddslagen. Undantag från rätten till dataportabilitet får i stället vid behov övervägas på sektorsspecifik nivå.

Löpande text som utgör utkast eller minnesanteckning ska inte omfattas av rätten till tillgång

Den registrerade har enligt 26 § första stycket PUL rätt att på begäran få information om och tillgång till de personuppgifter som behandlas, ett så kallat registerutdrag. Bestämmelsen genomför i svensk rätt artikel 12 a i dataskyddsdirektivet om rätten till tillgång. Rätten till tillgång innebär enligt EU-domstolen inte en rätt att få del av den handling där personuppgifterna förekommer, se dom YS mot Minister voor Immigratie, C-141/12, EU:C:2014:2081, punkt 58. I dataskyddsförordningen regleras rätten till tillgång i artikel 15 i dataskyddsförordningen. Denna rätt ska enligt artikel 15.4 inte inverka menligt på andra rättigheter och friheter.

I 26 § tredje stycket PUL föreskrivs undantag från rätten till tillgång. Enligt bestämmelsen behöver s.k. registerutdrag enligt 26 § första stycket inte lämnas om personuppgifter i löpande text som inte fått sin slutliga utformning när ansökan gjordes eller som utgör minnesanteckning eller liknande. Undantaget gäller dock inte om uppgifterna har lämnats ut till tredje man eller om uppgifterna behandlas enbart för historiska, statistiska eller vetenskapliga ändamål eller, när det gäller löpande text som inte fått sin slutliga utformning, om uppgifterna har behandlats under längre tid än ett år.

I förarbetena till detta undantag anges, bl.a. med hänvisning till regleringen i 2 kap. TF, att det på såväl den offentliga som den privata sidan finns goda skäl för en ordning som innebär att ofärdiga alster, minnesanteckningar och liknande inte behöver lämnas ut (prop. 1997/98:44 s. 83–84). Att under en rimlig tid få ha sina ofärdiga alster och minnesanteckningar i fred kan enligt förarbetena anses som en sådan fri- och rättighet som enligt artikel 13.1 i dataskyddsdirektivet berättigar till en begränsning av informationsskyldigheten. Av förarbetena framgår vidare att om uppgifterna behandlats under så lång tid som ett år utan att texten färdigställts, kan dock den registrerades intresse av att få ta del av sina uppgifter anses väga tyngre än den personuppgifts-

ansvariges intresse av att utan insyn få ytterligare fördröja färdigställandet av texten.

Detta resonemang är enligt regeringens mening fortfarande relevant. I förhållande till myndigheter behövs ett sådant undantag för att säkerställa de mål av allmänt intresse som det ankommer på myndigheter att värna. Dessa intressen utgör grund för undantag från de registrerades rättigheter, särskilt enligt artikel 23.1 e, f och h. I förhållande till den privata sektorn är undantaget nödvändigt bl.a. för att skydda enskildas fri- och rättigheter, vilket är en tillåten grund för undantag enligt artikel 23.1 i. Undantaget respekterar andemeningen i de grundläggande rättigheterna och friheterna och utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle.

Regeringen anser att det befintliga undantaget i 26 § tredje stycket PUL fyller sitt syfte och fungerar väl. Till skillnad från *dataskydd.net* anser regeringen att detta även gäller avgränsningen till löpande text. Det bör därför i dataskyddslagen tas in en bestämmelse som på motsvarande sätt gör undantag från rätten till tillgång enligt artikel 15 i dataskyddsförordningen avseende personuppgifter i löpande text som inte fått sin slutliga utformning när ansökan gjordes eller som utgör minnesanteckning eller liknande. Undantaget bör i likhet med gällande rätt inte gälla om uppgifterna har lämnats ut till tredje part eller om uppgifterna behandlas enbart för arkivändamål av allmänt intresse eller för statistiska ändamål eller, när det gäller löpande text som inte fått sin slutliga utformning, om uppgifterna har behandlats under längre tid än ett år. *Länsstyrelsen i Kronobergs län* uppfattar förslaget som att t.ex. utkast till beslut ska lämnas ut efter ett år. Regeringen vill dock i det sammanhanget betona att artikel 15 i dataskyddsförordningen inte ger den registrerade någon rätt att ta del av den handling där uppgifter om honom eller henne förekommer. Själva utkastet behöver således inte lämnas ut. Däremot ska den registrerade, på begäran, få tillgång till uppgifterna i handlingen och den information som anges i artikel 15, om behandlingen har pågått under längre tid än ett år. Regeringen anser inte att det framkommit skäl att förlänga denna tid, på det sätt som bl.a. *Svensk Försäkring* föreslår. Skulle ett sådant behov föreligga på ett visst område bör det regleras särskilt.

Regeringen ska få meddela ytterligare föreskrifter

Ytterligare undantag kan komma att behöva föreskrivas med stöd av artikel 23 i dataskyddsförordningen. Det kommer också att finnas behov av sådana undantag från de registrerades rättigheter som kan föreskrivas med stöd av artikel 89.2–3. Mot denna bakgrund bör det införas ett bemyndigande i dataskyddslagen som i sak motsvarar det bemyndigande som finns i 8 a § PUL. Regeringen anser, till skillnad från *Svensk Försäkring*, att det saknas skäl att införa en möjlighet att vidaredelegera rätten att meddela sådana föreskrifter till Datainspektionen.

14 Arkiv och statistik

14.1 Arkivändamål av allmänt intresse

14.1.1 Föreskrifter om arkiv ger stöd för behandling av personuppgifter

Regeringens bedömning: Myndigheter och andra som omfattas av föreskrifter om arkiv har enligt gällande rätt rättslig grund för behandling av personuppgifter för arkivändamål av allmänt intresse.

Vidarebehandling av personuppgifter för arkivändamål av allmänt intresse ska enligt EU:s dataskyddsförordning inte anses vara oförenlig med de ursprungliga ändamålen. Någon rättslig grund behöver inte fastställas för sådan vidarebehandling.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Det stora flertalet remissinstanser instämmer i utredningens bedömning eller kommenterar den inte. Enligt *Riksarkivet* ryms myndigheternas arkivering inom det ändamål för vilket uppgifterna ursprungligen samlas in. Riksarkivet anser därför att begreppet arkivändamål av allmänt intresse bör reserveras för den behandling som sker hos arkivinstitutioner. *Svenska kyrkan* påpekar att utredningen inte har behandlat frågan om huruvida Svenska kyrkans arkivändamål ska anses vara arkivändamål av allmänt intresse. *Skolverket* anger att även kommunala arkivmyndigheter tar över och förvarar enskilda arkiv. Skolverket anser att även denna verksamhet bör regleras.

Skälen för regeringens bedömning

Begreppet arkivändamål av allmänt intresse

I dataskyddsförordningen finns ett antal bestämmelser som särskilt rör personuppgiftsbehandling för arkivändamål av allmänt intresse. Enligt artikel 5.1 b gäller exempelvis att ytterligare behandling (vidarebehandling) av personuppgifter för sådana ändamål, i enlighet med artikel 89.1, inte ska anses oförenlig med de ursprungliga ändamålen. Av artikel 5.1 e följer att personuppgifter får lagras under en längre tid än vad som normalt gäller, om uppgifterna enbart kommer att behandlas för arkivändamål av allmänt intresse. Den förlängda bevarandetiden gäller under förutsättning att lämpliga tekniska och organisatoriska åtgärder vidtas i enlighet med kraven i artikel 89.1. I artikel 89.1 anges att behandling av personuppgifter för arkivändamål av allmänt intresse ska omfattas av lämpliga skyddsåtgärder i enlighet med förordningen för den registrerades rättigheter och friheter. Dessa skyddsåtgärder ska säkerställa att tekniska och organisatoriska åtgärder har införts för att se till att särskilt principen om uppgiftsminimering iakttas. Bestämmelsen är direkt tillämplig och riktar sig till den personuppgiftsansvarige. Detta utesluter dock inte att vissa skyddsåtgärder som avses i artikeln föreskrivs i författning.

Begreppet arkivändamål av allmänt intresse definieras inte i dataskyddsförordningen. I dataskyddsdirektivet används i stället begreppet

historiska ändamål. Det är oklart om någon skillnad i innebörd är avsedd. Den närmare innebörden av begreppet arkivändamål av allmänt intresse får därför klargöras i rättstillämpningen, särskilt i förhållande till begreppet historiska forskningsändamål som i dataskyddsförordningen ofta används i samma bestämmelser.

Svenska myndigheter, kommunala bolag och vissa andra organ är enligt arkivlagen (1990:782) skyldiga att bevara sina allmänna handlingar. Myndigheternas arkiv är enligt 3 § arkivlagen en del av det nationella kulturarvet och ska bevaras, hållas ordnade och vårdas så att de tillgodoser rätten att ta del av allmänna handlingar, behovet av information för rättskipningen och förvaltningen samt forskningens behov. Enligt regeringens mening står det klart att den behandling av personuppgifter som utförs för att uppfylla de krav som ställs i arkivlagen och anslutande föreskrifter måste anses ske för arkivändamål av allmänt intresse. Om begreppet skulle ha den snävare innebörd som *Riksarkivet* förespråkar, dvs. endast avse den behandling som sker av arkivmyndigheter, skulle det kunna ifrågasättas om myndigheter och andra organ skulle få ha interna arkiv för bevarande av uppgifter som inte längre behövs för det ursprungliga ändamålet. Detta kan inte vara avsikten med regleringen.

Föreskrifter om arkiv finns även på andra områden än inom den offentliga sektorn. Som *Svenska kyrkan* påpekar anges det i 12 § lagen om Svenska kyrkan att Svenska kyrkans arkiv ska bevaras, hållas ordnade och vårdas så att de tillgodoser rätten att ta del av kyrkans handlingar, behovet av information för rättskipning och förvaltning och forskningens behov. Regeringen gör bedömningen att behandling av personuppgifter som är nödvändig för att uppfylla sådan annan arkivlagstiftning, som på motsvarande sätt som arkivlagen syftar till att bevara och vårda en del av det svenska kulturarvet, också måste anses ske för arkivändamål av allmänt intresse.

Däremot anser regeringen, i likhet med utredningen, att behandling av personuppgifter som utförs för att uppfylla krav på bevarande för andra syften, såsom exempelvis kravet på arkivering av räkenskapsinformation enligt bokföringslagen (1999:1078), inte utgör behandling för arkivändamål av allmänt intresse. Det är dock en annan sak att det, när kravet på bevarande för andra syften inte längre kvarstår, kan finnas skäl att bevara även sådan information för arkivändamål av allmänt intresse, t.ex. för att arkivlagen kräver det.

Rättslig grund och tillåten vidarebehandling

Den behandling av personuppgifter som myndigheter och andra utför när de i enlighet med föreskrifter om arkiv arkiverar sina handlingar utgör en vidarebehandling som sker för arkivändamål av allmänt intresse. Behandlingen ska därmed enligt artikel 5.1 b inte anses som oförenlig med de ursprungliga ändamålen. Det krävs då inte någon annan rättslig grund än den med stöd av vilken insamlingen av personuppgifter medgavs (skäl 50).

Vidarebehandling är det bara fråga om när ett och samma organ, eller dennes personuppgiftsbiträde, utför ytterligare behandlingar avseende en viss uppgift. När en arkivmyndighet, t.ex. Riksarkivet, övertar arkiv-

material från en annan myndighet övergår hela ansvaret för det materialet till arkivmyndigheten (9 § tredje stycket arkivlagen). Den myndighet som har överlämnat materialet förfogar därefter inte längre över detta. Den myndigheten bestämmer inte heller längre över ändamålen och medlen för arkivmyndighetens behandling av de personuppgifter som förekommer i materialet. Arkivmyndigheten bär i stället personuppgiftsansvaret för de behandlingar som sker därefter (se definitionen av begreppet personuppgiftsansvarig i artikel 4.7 i dataskyddsförordningen).

Detta innebär att det behövs en rättslig grund för arkivmyndigheternas behandling av de personuppgifter som finns i det övertagna materialet. Den behandlingen sker för att utföra en i arkivlagstiftningen fastställd uppgift av allmänt intresse (se avsnitt 8.4). Nödvändig behandling hos arkivmyndigheterna kan därmed ske med dessa bestämmelser som rättslig grund, enligt artikel 6.1 e i dataskyddsförordningen. Detta gäller även t.ex. då Riksarkivet enligt 6 § andra stycket förordningen (2009:1593) med instruktion för Riksarkivet tar emot arkivhandlingar från enskilda som är av särskild betydelse för forskning och kulturarv.

Skolverket efterfrågar en reglering för kommunala arkivmyndigheter som övertar arkivmaterial från enskilda organ. Det finns inte något underlag för att i detta lagstiftningsärende bedöma behovet av en sådan reglering. Det kan dock konstateras att det i det enskilda fallet kan vara så att arkiven överlämnas till arkivmyndigheten som deposition, dvs. utan att äganderätten övergår. I sådana fall kan parterna avtala om att arkivmyndigheten ska ges ett privaträttsligt uppdrag att i egenskap av personuppgiftsbiträde förvara och vårda materialet för deponentens räkning.

14.1.2 Rättsligt stöd för behandling som utförs av enskilda arkivinstitutioner

Regeringens förslag: Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om att personuppgiftsansvariga som inte omfattas av föreskrifter om arkiv får behandla personuppgifter för arkivändamål av allmänt intresse. Den myndighet som regeringen bestämmer får även i enskilda fall tillåta sådan behandling. Ett beslut får förenas med villkor.

Utredningens förslag överensstämmer i sak med regeringens. Utredningen föreslår en annan språklig utformning av bestämmelsen.

Remissinstanserna: Det stora flertalet remissinstanser tillstyrker utredningens förslag eller har inga synpunkter på det. *Riksarkivet* ser behovet och nyttan av föreskrifter och beslut inom området, men efterfrågar ett förtydligande av förhållandet mellan de generella föreskrifterna och de förvaltningsbeslut som föreslås beslutas i enstaka fall, samt vad föreskrifterna i praktiken ska reglera. Vidare påpekar Riksarkivet att det inte framgår om de enskilda arkivens eller arkivinstitutionernas behandling av personuppgifter ska stå under Datainspektionens tillsyn. *Centrum för näringslivshistoria* betonar att det är av yttersta vikt att den här typen av bestämmelse införs. *Arbetarrörelsens arkiv och bibliotek* anför att det är av yttersta vikt att deras arbete inte försvåras eller omöjliggörs av ny

lagstiftning på området. *Föreningen svenska länsarkivarier* ställer sig bakom förslaget som en temporär lösning i avvaktan på regeringens utredning om arkivsektorn. Vidare anser föreningen att Riksarkivet är den givna myndigheten att hantera ett sådant ackrediteringsförfarande samt att det bör framgå att myndighetsutövningen ska ske i samråd med den enskilda arkivsektorn. *Dataskydd.net* anser däremot att Datainspektionen ska ha föreskriftsrätten i stället för Riksarkivet. *Datainspektionen* avstyrker förslaget och anser att bemyndigandet innebär att regeringen och Riksarkivet kan ge enskilda arkiv rätt att behandla personuppgifter för arkivändamål av allmänt intresse trots att en sådan uppgift inte är fastställd i nationell rätt. *Östergötlands läns landsting* anser att begreppet allmänt intresse bör definieras, särskilt i förhållande till enskilda arkivinstitutioner.

Skälen för regeringens förslag

Begreppet arkivändamål av allmänt intresse

Även de som inte omfattas av arkivlagstiftningen kan i vissa fall behandla personuppgifter för arkivändamål av allmänt intresse. Av skäl 158 till dataskyddsförordningen framgår att ett sådant organ bör ha en rättslig skyldighet att förvärva, bevara, bedöma, organisera, beskriva, kommunicera, främja, sprida och ge tillgång till uppgifter av bestående värde för allmänintresset. Medlemsstaterna bör enligt samma skäl ha rätt att föreskriva att personuppgifter får vidarebehandlas för arkivering, exempelvis i syfte att tillhandahålla specifik information om politiskt beteende under tidigare totalitära regimer, folkmord, brott mot mänskligheten, särskilt Förintelsen, eller krigsförbrytelser.

Östergötlands läns landsting anser att begreppet allmänt intresse bör definieras, särskilt i förhållande till enskilda arkivinstitutioner. Regeringen kan dock konstatera att begreppet är EU-rättsligt och inte kan definieras i nationell lagstiftning. Begreppet måste i stället ges utrymme att utvecklas i rättstillämpningen. Om syftet med behandlingen är just arkivändamål av allmänt intresse, och inte t.ex. historiska forskningsändamål, måste bedömas från fall till fall.

Rättsligt stöd för enskilda arkivorgans behandling av personuppgifter

Det finns i Sverige ett antal enskilda organ som samlar in eller vidarebehandlar personuppgifter för arkivändamål av allmänt intresse. Den rättsliga grunden för denna behandling torde i normalfallet vara att verksamheten är av allmänt intresse enligt 10 § d PUL. Det är dock oklart om uppgifterna för de enskilda arkivorgan, vilkas verksamhet är av allmänt intresse, alltid är fastställda i enlighet med svensk rätt på det sätt som krävs för att artikel 6.1 e i dataskyddsförordningen ska vara tillämplig. När dataskyddsförordningen börjar tillämpas kan därmed den rättsliga grunden för de enskilda organens behandling av personuppgifter komma att ifrågasättas. Det finns därför behov av att förtydliga det rättsliga stödet för sådan personuppgiftsbehandling.

Regeringen delar utredningens bedömning att detta bör ske genom att det införs en möjlighet för regeringen eller den myndighet som regeringen bestämmer att meddela föreskrifter som tillåter att person-

uppgiftsansvariga behandlar personuppgifter för arkivändamål av allmänt intresse. Till skillnad från *Datainspektionen* anser regeringen att en föreskrift som tillåter en personuppgiftsansvarig att behandla personuppgifter för arkivändamål av allmänt intresse ger det stöd i rättsordningen som behövs. En föreskrift som tillåter att t.ex. en förening behandlar personuppgifter för arkivändamål av allmänt intresse innebär i sig att föreningen erkänns ha befogenhet att bedriva arkivverksamhet av allmänt intresse. Därmed är en uppgift av allmänt intresse fastställd på det sätt som krävs enligt artikel 6.3 första stycket i dataskyddsförordningen.

Regeringen har för avsikt att delegera föreskriftsrätten till Riksarkivet, eftersom det är den myndighet som har bäst förutsättningar att bedöma vilka kriterier som ska vara uppfyllda för att en arkivverksamhet ska anses vara av allmänt intresse i dataskyddsförordningens mening. Riksarkivet bör dock ha en skyldighet att höra Datainspektionen innan föreskrifter meddelas. Vidare bör Riksarkivet vid behov inhämta synpunkter från den enskilda arkivsektorn i allmänhet och de berörda personuppgiftsansvariga i synnerhet.

Med anledning av *Riksarkivets* önskemål om förtydligande av vad föreskrifterna i praktiken ska reglera kan regeringen nämna att föreskrifterna skulle kunna innehålla generella bestämmelser som bör gälla för all arkivverksamhet av allmänt intresse som inte omfattas av arkivlagstiftningen, i linje med vad som anges i skäl 158. De berörda personuppgiftsansvariga skulle kunna anges i en bilaga till föreskrifterna, med angivande av den verksamhet som bedöms vara av allmänt intresse. I förekommande fall kan begränsningar avseende de generella bestämmelserna eller särskilda villkor för tillämpningen anges. Den närmare utformningen av föreskrifterna och innehållet i dessa bör dock överlämnas till Riksarkivet att bestämma.

Det är tänkbart att det kan uppstå enstaka situationer där föreskriftsformen inte är lämplig, men där det ändå finns skäl att tillåta behandling av personuppgifter för arkivändamål av allmänt intresse. Det kan t.ex. röra sig om behandling som ska ske av en personuppgiftsansvarig under en begränsad tid eller i ett mycket begränsat avseende. I likhet med den ordning som gäller för behandling av personuppgifter om lagöverträdelser som föreslås i avsnitt 11, bör därför den myndighet som regeringen bestämmer i enskilda fall kunna pröva om den behandling som utförs sker för arkivändamål av allmänt intresse i dataskyddsförordningens mening. Regeringen har för avsikt att ge Riksarkivet även denna uppgift. Om Riksarkivet bedömer att sökandens arkivverksamhet uppfyller dataskyddsförordningens krav kan denna genom ett särskilt beslut medges rätt att behandla personuppgifter för arkivändamål av allmänt intresse. Den personuppgiftsbehandling som är nödvändig för detta ändamål kan då ske med beslutet som rättslig grund. Ett beslut som går sökanden emot bör kunna överklagas, se avsnitt 17.5.

Riksarkivet påpekar att det i betänkandet inte framgår om Datainspektionen ska utöva tillsyn över de enskilda arkivens eller arkivinstitutionernas behandling av personuppgifter. Regeringen kan i det sammanhanget nämna att regeringen har för avsikt att, i förordning, utse Datainspektionen som tillsynsmyndighet enligt dataskyddsförordningen. All behandling av personuppgifter som sker inom dataskyddsförord-

ningens och dataskyddslagens tillämpningsområde kommer att omfattas av Datainspektionens tillsyn, oavsett vilken den rättsliga grunden för behandlingen är. Det innebär således, precis som i dag, att en enskild arkivinstitution som förvarar handlingar som innehåller personuppgifter kommer att stå under Datainspektionens tillsyn. Detta gäller oavsett om behandlingen utförs med stöd av Riksarkivets föreskrifter eller beslut, på grund av att behandlingen sker för arkivändamål av allmänt intresse, eller om organet genom ett civilrättsligt avtal med arkivmaterialets ägare endast behandlar personuppgifterna i egenskap av personuppgiftsbiträde åt deponenten.

Regeringen har tidigare bedömt att det finns anledning att genomföra en bred översyn av arkivväsendet i landet och att denna översyn även ska tydliggöra de enskilda arkivens viktiga roll som en del av det gemensamma kulturarvet (prop. 2016/17:116 s. 174–175). Utredningen förutsätter mot denna bakgrund att frågor kring de enskilda arkivens behandling av personuppgifter kommer att utredas närmare. En sådan översyn av arkivväsendet har nu inletts. Enligt regeringens kommittédirektiv, dir. 2017:106, ska en särskild utredare bl.a. analysera om regleringen för de enskilda arkiven bör förändras för att kunna tillgodose behov inom rättsskipning, förvaltning, forskning och skydd för kulturarvet. Utredaren ska även utreda om de enskilda arkivens hantering av personuppgifter kräver ytterligare författningsstöd samt analysera Riksarkivets och övriga arkivmyndigheters roll och uppgifter i relation till de enskilda arkiven och vid behov lämna förslag på hur dessa kan förändras. Precis som *Föreningen svenska länsarkivarier* påpekar kan därför den ordning som föreslås i detta lagstiftningsärende avseende enskildas behandling av personuppgifter för arkivändamål av allmänt intresse komma att bli en övergångslösning.

14.1.3 Behandling av bland annat känsliga personuppgifter för arkivändamål

Regeringens förslag: Känsliga personuppgifter och personuppgifter som rör lagöverträdelser får behandlas om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna följa föreskrifter om arkiv.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om att personuppgiftsansvariga som inte omfattas av föreskrifter om arkiv får behandla känsliga personuppgifter för arkivändamål av allmänt intresse. Den myndighet som regeringen bestämmer får även i enskilda fall tillåta sådan behandling. Ett beslut får förenas med villkor.

Utredningens förslag överensstämmer i sak med regeringens. Utredningen föreslår en annan språklig utformning av bestämmelsen.

Remissinstanserna: Det stora flertalet remissinstanser tillstyrker utredningens förslag eller har inga synpunkter på det. *Centrum för näringslivshistoria* anför att det är av yttersta vikt att den här typen av bestämmelse införs. *Arbetarrörelsens arkiv och bibliotek* anför att det är av yttersta vikt att deras arbete inte försvåras eller omöjliggörs av ny

lagstiftning på området. *Föreningen svenska länsarkivarier* ställer sig bakom förslaget som en temporär lösning i avvaktan på regeringens utredning om arkivsektorn. Vidare anser föreningen att Riksarkivet är den givna myndigheten att hantera ett sådant ackrediteringsförfarande samt att det bör framgå att myndighetsutövningen ska ske i samråd med den enskilda arkivsektorn. *Dataskydd.net* anser i stället att Datainspektionen ska ha föreskriftsrätten. Vidare anser dataskydd.net att bestämmelsen som rör sådan behandling av känsliga personuppgifter som är nödvändig för att följa föreskrifter om arkiv ska tas bort och att bestämmelsen om sådan behandling av personuppgifter som rör lagöverträdelser ska kompletteras med ett krav på dokumentation, om pseudonymiserade uppgifter inte kan användas vid arkiveringen. *Pensionsmyndigheten* anser inte att det är självklart att förordningen ska tolkas så att det finns ett behov av att i dataskyddslagen eller i annan nationell lagstiftning ta in bestämmelser om undantag från förbudet att behandla känsliga personuppgifter. Om sådana bestämmelser beslutas anser myndigheten att detta inte bör ske utan ett förtydligande av det av utredningen använda uttrycket föreskrifter om bevarande och vård av arkiv. Även *Centrala studiestödsnämnden* anser det vara av vikt att det fortsatta lagstiftningsarbetet tydliggör vilka delar av arkivlagstiftningen som formuleringen om föreskrifter om bevarande och vård av arkiv syftar på. *Datainspektionen* anser att utredningen inte har visat att det skydd som finns i dag i nationell lagstiftning för myndigheters arkiv uppfyller kraven på lämpliga skyddsåtgärder.

Skälen för regeringens förslag

Myndigheter och andra organ som omfattas av föreskrifter om arkiv

Bestämmelsen i 8 § andra stycket PUL tydliggör att personuppgiftslagen inte hindrar att en myndighet arkiverar och bevarar allmänna handlingar eller att arkivmaterial tas om hand av en arkivmyndighet. Bestämmelsen innebär bl.a. att känsliga personuppgifter kan behandlas trots förbudet i 13 § PUL (prop. 1997/98:44 s. 47–48). I praktiken innebär bestämmelsen i 8 § andra stycket PUL att arkivlagstiftningen har företräde framför personuppgiftslagen. Detta är en nödvändig utgångspunkt för att den svenska offentlighetsprincipen fullt ut ska kunna fylla sin funktion. Det finns ingenting i dataskyddsförordningen som förhindrar att ett sådant synsätt bibehålls. Tvärtom säkerställs, som utvecklas i avsnitt 7.1, offentlighetsprincipens ställning genom artikel 86 i förordningen.

I artikel 9.1 i dataskyddsförordningen anges att behandling som avslöjar känsliga personuppgifter ska vara förbjuden, se avsnitt 10.1. Utrymmet för undantag från detta förbud, vid behandling som är nödvändig för arkivändamål av allmänt intresse, regleras i artikel 9.2 j. Där anges att förbudet inte gäller om behandlingen är nödvändig för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1, på grundval av unionsrätten eller medlemsstaternas nationella rätt, vilken ska stå i proportion till det eftersträvade syftet, vara förenlig med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.

För att behandling av känsliga personuppgifter ska vara tillåten för arkivändamål i allmänt intresse krävs således att unionsrätten eller den nationella rätten innehåller bestämmelser om lämpliga och särskilda åtgärder. Detta krav överensstämmer med det som gäller för behandling av känsliga personuppgifter med hänsyn till andra viktiga allmänna intressen enligt artikel 9.2 g i dataskyddsförordningen. Kraven på lämpliga och särskilda åtgärder i artikel 9.2 g och j i dataskyddsförordningen motsvarar det krav på skyddsåtgärder som ställs enligt dataskyddsdirektivet. Kravet på lämpliga och särskilda åtgärder i dataskyddsförordningen innebär således ingen ny begränsning av möjligheten att behandla känsliga personuppgifter för arkivändamål av allmänt intresse.

Den nödvändiga behandling av personuppgifter som sker vid arkiv som omfattar allmänna handlingar har rättslig grund i arkivlagen och anslutande föreskrifter. Regeringen konstaterar i avsnitt 10.4 att svensk rätt innehåller lämpliga och särskilda åtgärder som skyddar enskildas integritet vid hanteringen av allmänna handlingar, t.ex. i form av sekretess, rätt till partsinsyn och föreskrifter om informationssäkerhet och gallring. I synnerhet de nationella författningsbestämmelserna om sekretess utgör en sådan lämplig och särskild åtgärd som avses i artikel 9.2 g och j, eftersom dessa har utformats noggrant efter en avvägning mellan behovet av skydd och intresset av insyn.

Regeringen anser mot denna bakgrund, till skillnad från *Datainspektionen*, att det skydd som enligt svensk rätt gäller för myndigheters arkiv uppfyller kraven på lämpliga och särskilda åtgärder. Enligt regeringens bedömning kan därmed även känsliga personuppgifter behandlas då det är nödvändigt för att följa föreskrifter om arkiv, med stöd av artikel 9.2 j i dataskyddsförordningen.

Till skillnad från *dataskydd.net* anser dock regeringen att dataskyddslagen bör innehålla en uttrycklig bestämmelse som, i likhet med 8 § andra stycket första meningen PUL, tydliggör att en myndighet får arkivera och bevara allmänna handlingar som innehåller känsliga personuppgifter samt att arkivmaterial som innehåller känsliga personuppgifter får tas om hand av en arkivmyndighet.

Utredningen föreslår att känsliga personuppgifter ska få behandlas om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna följa föreskrifter om bevarande och vård av arkiv. Av *Pensionsmyndighetens* och *Centrala studiestödsnämndens* remissyttranden framgår att denna formulering skulle kunna förstås på så sätt att den endast syftar på vissa delar av arkivlagstiftningen. Enligt regeringen bör bestämmelsen därför i stället ange att känsliga personuppgifter får behandlas om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna följa föreskrifter om arkiv. Bestämmelsen förtydligar bl.a. att dataskyddsförordningen och dataskyddslagen inte hindrar att allmänna handlingar arkiveras och bevaras eller att arkivmaterial tas om hand av en arkivmyndighet. Den författningstekniska skillnaden mellan 8 § andra stycket första meningen PUL och den bestämmelse som regeringen föreslår innebär således ingen saklig förändring i denna del.

Arkivlagen och andra föreskrifter om arkiv omfattar inte bara myndigheter utan även t.ex. kommunala bolag och vissa andra utpekade enskilda organ. För dessa skulle det i enstaka fall kunna uppstå en normkonflikt mellan arkivlagstiftningen och regleringen i artikel 10 i dataskydds-

förordningen avseende behandlingen av personuppgifter som rör lagöverträdelser (se avsnitt 11). Dataskyddslagen bör därför även innehålla en bestämmelse som, på motsvarande sätt som avseende känsliga personuppgifter, tillåter behandling av personuppgifter som rör lagöverträdelser, om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna följa föreskrifter om arkiv. Bestämmelsen bör inte förenas med ett sådant krav på dokumentation som dataskydd.net förespråkar.

Personuppgiftsansvariga som inte omfattas av föreskrifter om arkiv

Även hos personuppgiftsansvariga som inte omfattas av föreskrifter om arkiv kan det finnas ett allmänt intresse av att känsliga personuppgifter bevaras. Sådant bevarande bör enligt regeringens bedömning också tillåtas under vissa förutsättningar. Risken är annars uppenbar att viktig information om vår samtid går förlorad. Det bör därför införas en bestämmelse i dataskyddslagen som anger att regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter som tillåter att personuppgiftsansvariga som inte omfattas av föreskrifter om arkiv får behandla känsliga personuppgifter för arkivändamål av allmänt intresse. Regeringen har för avsikt att delegera föreskriftsrätten till Riksarkivet. Riksarkivet bör även i enskilda fall få besluta att personuppgiftsansvariga får behandla sådana personuppgifter för arkivändamål av allmänt intresse. Sådana föreskrifter och förvaltningsbeslut bör lämpligen meddelas i samband med att den rättsliga grunden fastställs för den personuppgiftsansvariges behandling av personuppgifter för arkivändamål av allmänt intresse, se föregående avsnitt. Förvaltningsbeslut kan även meddelas som komplement till en tidigare antagen föreskrift som ger den personuppgiftsansvarige rättslig grund för behandling av personuppgifter för detta ändamål.

För enskilda arkiv finns det inte några generella föreskrifter om lämpliga och särskilda åtgärder, utöver dem som följer direkt av dataskyddsförordningen och den som regeringen föreslår i följande avsnitt. Mot bakgrund av att de enskilda arkiven sinsemellan uppvisar stora olikheter är det heller inte lämpligt att i lag slå fast att en viss typ av ytterligare åtgärd alltid ska gälla vid behandling av känsliga personuppgifter. Det bör i stället ankomma på Riksarkivet att, efter samråd med Datainspektionen, bedöma om beslut som tillåter ett enskilt organ att behandla känsliga personuppgifter ska villkoras av att den personuppgiftsansvarige vidtar särskilda åtgärder och i så fall vilka. Det kan t.ex. röra sig om åtkomstbegränsningar, krav på särskilda tekniska säkerhetsåtgärder eller någon annan åtgärd som bedöms lämplig och proportionerlig i det aktuella fallet.

14.1.4 Användningsbegränsning

Regeringens förslag: Personuppgifter som behandlas enbart för arkivändamål av allmänt intresse får användas för att vidta åtgärder i fråga om den registrerade endast om det finns synnerliga skäl med hänsyn till den registrerades vitala intressen. Denna begränsning hindrar inte myndigheter och andra vars verksamhet omfattas av offentlighetsprincipen och sekretesslagstiftningen från att använda personuppgifter som finns i allmänna handlingar.

Utredningens förslag överensstämmer i sak med regeringens. Utredningens förslag har en annan språklig utformning.

Remissinstanserna: Det stora flertalet remissinstanser tillstyrker utredningens förslag eller har inga synpunkter på det. *E-hälsomyndigheten* saknar ett förtydligande av om uttrycket vitala intressen ska uppfattas på ett annat sätt än uttrycket intressen som är av grundläggande betydelse. *Konkurrensverket* efterlyser ett förtydligande kring innebörden av bestämmelsen. *Dataskydd.net* anser att ordet enbart introducerar en oklarhet och dramatiskt utökar myndigheternas befogenheter att behandla personuppgifter på ett för privatpersonen oönskat sätt. Vidare anser dataskydd.net att undantaget med hänsyn till vitala intressen ska tas bort. *Datainspektionen* anser att utredningen inte har visat att det skydd som finns i dag i nationell lagstiftning för myndigheters arkiv uppfyller kraven på lämpliga skyddsåtgärder.

Skälen för regeringens förslag: I 9 § fjärde stycket PUL anges att personuppgifter som behandlas för historiska, statistiska eller vetenskapliga ändamål får användas för att vidta åtgärder i fråga om den registrerade bara om den registrerade har lämnat sitt samtycke eller det finns synnerliga skäl med hänsyn till den registrerades vitala intressen. Enligt 8 § andra stycket PUL gäller dock denna begränsning inte för en myndighets användning av personuppgifter i allmänna handlingar.

När en personuppgift inte längre behöver behandlas för det ursprungliga ändamålet ska den, enligt huvudregeln i artikel 5.1 e i dataskyddsförordningen, gallras eller anonymiseras. Undantag gäller dock om det finns ett arkivändamål av allmänt intresse. Möjligheten till förlängd bevarandetid förutsätter att uppgiften enbart behandlas för arkivändamål. Det kan emellertid inte uteslutas att en arkiverad uppgift åter kan komma att behövas även för andra ändamål, t.ex. i den personuppgiftsansvariges kärnverksamhet. Begränsningen i 9 § fjärde stycket PUL förhindrar sådan återanvändning i vissa situationer, oavsett om den nya behandlingen ska ske för det ursprungliga insamlingsändamålet eller för något annat därmed förenligt ändamål. Av förarbetena till bestämmelsen framgår dock att bestämmelsen inte aktualiseras om en arkiverad uppgift även behandlas för andra ändamål, dvs. inte enbart för arkivändamål (SOU 1997:39 s. 356–357). En uppgift som fortfarande behövs i kärnverksamheten och därför behandlas där kan alltså användas för att vidta åtgärder i fråga om den registrerade, även om samma uppgift också förekommer i en arkiverad handling hos den personuppgiftsansvarige.

Utredningen föreslår att en bestämmelse som i sak motsvarar 9 § fjärde stycket PUL ska införas i dataskyddslagen. Regeringen anser, till skillnad från *dataskydd.net*, att detta utgör en väl avvägd skyddsåtgärd. Precis

som i personuppgiftslagen bör bestämmelsen inte bara avse känsliga personuppgifter. Den nya bestämmelsen bör dock, som utredningen föreslår, utformas så att det tydligare än i dag framgår att användningsbegränsningen bara gäller personuppgifter som enbart behandlas för arkivändamål av allmänt intresse. Det är så bestämmelsen i personuppgiftslagen är avsedd att tillämpas och tillägget utgör därmed inte, som dataskydd.net anger, någon utvidgning av den personuppgiftsansvariges befogenheter. Det finns vidare inte skäl att ange i paragrafen att uppgifter får användas med den registrerades samtycke. Om samtycke inhämtas till att en arkiverad uppgift används för nya ändamål, kan behandlingen nämligen jämställas med personuppgiften samlas in på nytt med stöd av artikel 6.1 a i dataskyddsförordningen.

Personuppgifter som behandlas enbart för arkivändamål av allmänt intresse bör således få användas för att vidta åtgärder i fråga om den registrerade endast om det finns synnerliga skäl med hänsyn till den registrerades vitala intressen. Någon saklig skillnad mellan förslaget och 9 § fjärde stycket PUL är inte avsedd. Förarbeten och praxis avseende bestämmelsen i personuppgiftslagen bör därmed kunna vara vägledande även vid tillämpningen av dataskyddslagen. Detta medför även att det saknas skäl att, som *E-hälsomyndigheten* efterfrågar, utveckla förhållandet mellan begreppet vitala intressen och begreppet intressen som är av grundläggande betydelse.

Som framgår av föregående avsnitt anser regeringen, till skillnad från *Datainspektionen*, att den lagstiftning som rör hanteringen av allmänna handlingar innehåller lämpliga och särskilda åtgärder som skyddar enskildas integritet. Ytterligare skyddsåtgärder hos myndigheter, t.ex. i form av användningsbegränsningar som förhindrar återanvändning av arkiverade uppgifter, bör vid behov införas i sektorsspecifika författningar och inte i den generella lagen. Den föreslagna bestämmelsen om begränsningar av möjligheten att vidta åtgärder i fråga om den registrerade ska därför inte hindra myndigheter från att använda personuppgifter som finns i allmänna handlingar. Förslaget medför därmed ingen förändring i förhållande till vad som gäller enligt personuppgiftslagen. Med anledning av *Konkurrensverkets* önskemål om förtydligande kan regeringen således konstatera att användningsbegränsningen inte aktualiseras för myndigheternas del, eftersom en handling blir allmän senast i samband med att den omhändertas för arkivering. I likhet med utredningens förslag bör detta undantag från användningsbegränsningen gälla även för andra än myndigheter, i den mån bestämmelserna i tryckfrihetsförordningen och offentlighets- och sekretesslagen om allmänna handlingar och sekretess gäller i deras verksamhet.

14.1.5 Undantag från vissa av den registrerades rättigheter

Regeringens bedömning: Dataskyddslagen bör inte innehålla några generella undantag från den registrerades rättigheter vid behandling av personuppgifter för arkivändamål av allmänt intresse.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Det stora flertalet remissinstanser instämmer i utredningens bedömning eller kommenterar den inte. *Domstolsverket* påpekar att det i betänkandet saknas en förklaring till varför utredningen valt att undanta enbart arkivmyndigheternas personuppgiftsbehandling och inte all personuppgiftsbehandling för arkivändamål av allmänt intresse. *Skolverket* anser att undantag från rätten till rättelse och rätten att göra invändningar bör gälla hos alla myndigheter, vid behandling som enbart sker för arkivändamål av allmänt intresse. *Lunds universitet* föreslår att de undantag som görs rörande arkivmaterial som tagits emot för förvaring av myndigheten utsträcks till att gälla för alla typer av myndigheter med arkivfunktioner, inte bara till arkivmyndigheter. *Arbetsmiljöverket* anser att allmänna handlingar som omhändertagits för arkivering av en arkivmyndighet eller en arkivfunktion inom en myndighet, ska undantas från rätten till rättelse och begränsning av behandling av personuppgifter. *Stockholms kommun* anser att undantag från de registrerades rättigheter bör gälla även för övriga offentliga myndigheter som förvaltar och lagrar äldre arkiv och inte bara gälla levererat material till arkivmyndighet utan även avslutade arkiv som förvaras hos myndigheter.

Skälen för regeringens bedömning: Dataskyddsförordningen innehåller i artikel 14.5 b och 17.3 d vissa direkt tillämpliga undantag från de registrerades rättigheter vid behandling av personuppgifter för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål. Om personuppgifter behandlas för arkivändamål av allmänt intresse får det enligt artikel 89.3 i dataskyddsförordningen dessutom föreskrivas undantag från de rättigheter som avses i artiklarna 15, 16, 18, 19, 20 och 21, med förbehåll för de villkor och skyddsåtgärder som avses i artikel 89.1 (se avsnitt 14.1.1). Detta får emellertid bara göras i den utsträckning som sådana rättigheter sannolikt kommer att göra det omöjligt eller mycket svårare att uppfylla de särskilda ändamålen och sådana undantag krävs för att uppnå detta ändamål. Utredningen föreslår att vissa sådana undantag ska införas i arkivförordningen (1991:446), när det gäller personuppgifter i arkivmaterial som tagits emot för förvaring av en arkivmyndighet. Några remissinstanser, bl.a. *Skolverket*, *Lunds universitet* och *Stockholms kommun*, anser dock att dessa undantag från de registrerades rättigheter inte bara ska gälla hos arkivmyndigheterna, utan även hos andra myndigheter som behandlar personuppgifter för arkivändamål av allmänt intresse.

Som utredningen påpekar är väl fungerande myndighetsarkiv av grundläggande betydelse för forskning och utveckling, insyn och delaktighet, ansvarsutkrävande och demokrati. Detta intresse kan i vissa situationer väga tyngre än den enskildes intresse av att kunna utöva sina rättigheter enligt dataskyddsförordningen. Regeringens allmänna utgångspunkt är dock att dataskyddslagen inte bör inskränka de registrerades rättigheter i större utsträckning än vad som gäller enligt personuppgiftslagen. Eftersom det i personuppgiftslagen inte finns några generella undantag från de registrerades rättigheter vid behandling av personuppgifter för historiska ändamål bör några undantag vid behandling för arkivändamål av allmänt intresse inte heller införas i dataskyddslagen.

14.2 Statistiska ändamål

Regeringens förslag: Känsliga personuppgifter får behandlas för statistiska ändamål, om samhällsintresset av det statistikprojekt där behandlingen ingår klart väger över den risk för otillbörligt intrång i enskildas personliga integritet som behandlingen kan innebära.

Personuppgifter som enbart behandlas för statistiska ändamål får användas för att vidta åtgärder i fråga om den registrerade endast om det finns synnerliga skäl med hänsyn till den registrerades vitala intressen. Användningsbegränsningen gäller även för myndigheters användning av statistikuppgifter som finns i allmänna handlingar.

Utredningens förslag överensstämmer i sak med regeringens. Utredningens förslag har en annan språklig utformning.

Remissinstanserna: Det stora flertalet remissinstanser tillstyrker utredningens förslag eller har inga synpunkter på det. *Svensk Försäkring* menar att möjligheten att vidarebehandla uppgifter för statistikändamål bör vidgas. *Tjänstemännens centralorganisation* efterfrågar exempel på sådant som kan vara av stort samhällsintresse och anser att lönestatistikprojekt bör vara ett sådant. *Statistiska centralbyrån* anför att byråns behandling av personuppgifter i samband med uppdrag åt forskare bör betraktas som behandling av personuppgifter för statistiska ändamål. *Migrationsverket* anser att det är ett väl avvägt förslag att myndigheter inte ska få använda statistikuppgifter för åtgärder mot den registrerade. *E-hälsomyndigheten* saknar ett förtydligande av om uttrycket vitala intressen ska uppfattas på ett annat sätt än uttrycket intressen som är av grundläggande betydelse. *Dataskydd.net* anser att ordet enbart introducerar en oklarhet och dramatiskt utökar myndigheternas befogenheter att behandla personuppgifter på ett för privatpersonen oönskat sätt. Vidare anser dataskydd.net att undantaget med hänsyn till vitala intressen ska tas bort.

Skälen för regeringens förslag

Behandling av personuppgifter för statistiska ändamål

I dataskyddsförordningen avses med statistiska ändamål varje åtgärd som vidtas för den insamling och behandling av personuppgifter som är nödvändig för statistiska undersökningar eller för framställning av statistiska resultat (skäl 162). Ett statistiskt ändamål innebär, enligt samma skäl, att resultatet av behandlingen inte består av personuppgifter, utan av aggregerade personuppgifter, och att resultatet eller uppgifterna inte används till stöd för åtgärder eller beslut som avser en särskild privatperson.

Behandling av personuppgifter för statistiska ändamål förekommer inom såväl offentlig som privat sektor, både som en självständig verksamhet och som en uppföljande åtgärd till annan verksamhet. Statistiska undersökningar kan också utgöra en integrerad del av ett forskningsprojekt. Som *Statistiska centralbyrån* anför bör byråns behandling av personuppgifter i samband med uppdrag åt forskare betraktas som behandling av personuppgifter för statistiska ändamål. Däremot bör sådan behandling av personuppgifter för statistiska ändamål som utförs under forskarens ansvar bedömas enligt de bestämmelser som gäller vid

behandling för forskningsändamål. Vad som ryms inom begreppet forskning har behandlats av Forskningsdatautredningen, vars betänkande nu bereds inom Regeringskansliet (SOU 2017:50). Detta lagstiftningsärende omfattar således inte sådan behandling av personuppgifter för statistiska ändamål som sker i verksamhet som utgör forskning enligt dataskyddsförordningen.

Framställningen av den officiella statistiken, som ska finnas för allmän information, utredningsverksamhet och forskning, regleras av lagen (2001:99) om den officiella statistiken och förordningen (2001:100) om den officiella statistiken. Dessa författningar reglerar bl.a. under vilka förutsättningar känsliga personuppgifter får behandlas och vilken information som den statistikansvariga myndigheten ska lämna. De ändringar som dataskyddsförordningen föranleder i dessa författningar behandlas inte i detta lagstiftningsärende.

Den officiella statistiken och annan reglerad statistik framställs av särskilt utpekade myndigheter, som genom författning har tilldelats en uppgift av allmänt intresse. Personuppgifter kan således samlas in och i övrigt behandlas för detta ändamål, utan samtycke från de registrerade, med stöd av artikel 6.1 e i dataskyddsförordningen. Detsamma bör enligt regeringens mening gälla vid sådan statistikverksamhet som är nödvändig för att t.ex. en myndighet ska kunna utföra sitt fastställda uppdrag, även om statistik inte uttryckligen nämns i uppdraget (jfr avsnitt 8.4).

Behandling av personuppgifter inom ramen för ett statistikprojekt som inte är nödvändigt för att utföra en fastställd uppgift av allmänt intresse och som inte heller i sig utgör en sådan uppgift kan däremot inte ske med stöd av artikel 6.1 e i dataskyddsförordningen. Rättslig grund för behandlingen måste då sökas någon annanstans. I vissa fall kan insamling av personuppgifter för statistiska ändamål ske med stöd av samtycke från de registrerade. I andra fall, utom när myndigheter fullgör sina uppgifter, kan insamling av personuppgifter för viss statistikverksamhet vara tillåten utan samtycke, med stöd av en intresseavvägning enligt artikel 6.1 f i dataskyddsförordningen.

Det är mycket vanligt att personuppgifter som ursprungligen har samlats in för andra ändamål vidarebehandlas för statistiska ändamål, t.ex. som ett led i den personuppgiftsansvariges uppföljning av sin egentliga verksamhet. Sådan vidarebehandling är särskilt gynnad i dataskyddsförordningen, precis som i personuppgiftslagen. Uppgifter som ursprungligen har samlats in för något annat ändamål kan alltså även i fortsättningen användas för statistiska ändamål, utan att denna nya behandling anses vara oförenlig med de ursprungliga ändamålen (artikel 5.1 b i dataskyddsförordningen), under förutsättning att lämpliga tekniska och organisatoriska åtgärder vidtas i enlighet med kraven i artikel 89.1. En nyhet jämfört med personuppgiftslagen är att det vid sådan vidarebehandling inte krävs någon annan separat rättslig grund än den med stöd av vilken insamlingen av personuppgifter medgavs (skäl 50).

Behandling av känsliga personuppgifter

Känsliga personuppgifter får enligt artikel 9.2 j i dataskyddsförordningen behandlas för statistiska ändamål på grundval av unionsrätten eller medlemsstaternas nationella rätt, vilken ska stå i proportion till det eftersträvade syftet, vara förenlig med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen. Denna bestämmelse aktualiseras både vid insamling av känsliga personuppgifter för statistiska ändamål och vid vidarebehandling av känsliga personuppgifter för sådana ändamål.

Kravet på lämpliga och särskilda åtgärder överensstämmer med det som gäller för behandling av känsliga personuppgifter med hänsyn till andra viktiga allmänna intressen enligt artikel 9.2 g i dataskyddsförordningen. Dessa krav motsvarar i sin tur det krav på skyddsåtgärder som ställs i dataskyddsdirektivet om viktiga allmänna intressen, som legat till grund för personuppgiftslagens bestämmelser om behandling av personuppgifter för statistiska ändamål. Detta innebär att förutsättningarna för att det ska vara tillåtet att behandla känsliga personuppgifter för statistiska ändamål i huvudsak är desamma som enligt dataskyddsdirektivet.

Vidarebehandling av personuppgifter för statistiska ändamål ska enligt artikel 5.1 b i dataskyddsförordningen visserligen inte anses vara oförenlig med de ursprungliga ändamålen. Det kan däremot inte tas för givet att känsliga personuppgifter kan vidarebehandlas för statistiska ändamål enbart på grundval av det undantag från förbudet som tillämpats vid behandling enligt det ursprungliga ändamålet. Detta följer av att artikel 9.2 j i förordningen förutsätter att gällande rätt innehåller bestämmelser om lämpliga och särskilda skyddsåtgärder för att säkerställa den registrerades rättigheter och intressen.

Enligt 19 § andra stycket PUL får känsliga personuppgifter behandlas för statistikändamål, om behandlingen är nödvändig på sätt som sägs i 10 § och om samhällsintresset av det statistikprojekt där behandlingen ingår klart väger över den risk för otillbörligt intrång i enskildas personliga integritet som behandlingen kan innebära. I 19 § tredje stycket PUL anges att förutsättningarna enligt andra stycket ska anses uppfyllda om behandlingen har godkänts av en forskningsetisk kommitté, dvs. ett sådant särskilt organ för prövning av forskningsetiska frågor som har företrädare för såväl det allmänna som forskningen och som är knutet till ett universitet eller en högskola eller till någon annan instans som i mera betydande omfattning finansierar forskning.

I förarbetena till 19 § andra stycket PUL anges att viss statistik är så viktig att den inte bör vara beroende av att varje berörd enskild har informerats och lämnat sitt samtycke (prop. 1997/98:44 s. 71). Vidare framgår att det mot bakgrund av att det finns många olikartade statistikprojekt, vilka som regel pågår bara under en begränsad tid, förefaller lämpligare att göra en avvägning i varje särskilt fall än att i lag införa generella regler om vilken statistik som ska tillåtas. Vid en sådan individuell avvägning kan olika faktorer kring projektet, t.ex. hur pass viktig den kunskap är som projektet kan ge, vägas mot intrånget i den enskildes personliga integritet.

Regeringen anser att det inte heller nu är lämpligt att genom lagstiftning på förhand avgöra exakt i vilka fall behandling av känsliga personuppgifter ska få ske för statistiska ändamål. I enlighet med utredningens förslag bör det därför i dataskyddslagen införas en avvägningsnorm motsvarande den som finns i 19 § andra stycket PUL. Behandling av känsliga personuppgifter för statistiska ändamål ska således få ske om samhällsintresset av det statistikprojekt där behandlingen ingår klart väger över den risk för otillbörligt intrång i enskildas personliga integritet som behandlingen kan innebära. Detta villkor för behandling utgör en sådan lämplig och särskild åtgärd som avses i artikel 9.2 j i dataskyddsförordningen. Med anledning av *Tjänstemännens centralorganisations* önskemål om exempel på sådant som kan vara av stort samhällsintresse, kan konstateras att den praxis som finns avseende tillämpningen av 19 § andra stycket PUL bör kunna tjäna som vägledning för tillämpningen även av den föreslagna bestämmelsen. För att bestämmelsen ska aktualiseras förutsätts givetvis att insamlingen av personuppgifter är tillåten med stöd av någon av de rättsliga grunderna i artikel 6.1 i dataskyddsförordningen eller att behandlingen utgör en tillåten vidarebehandling av för andra ändamål insamlade personuppgifter.

Som nämns ovan anser regeringen att sådana statistiska undersökningar som utgör en integrerad del av ett forskningsprojekt ska bedömas enligt de bestämmelser som gäller för behandling av personuppgifter för forskningsändamål. Den avvägningsnorm som föreslås här kommer därmed endast att vara tillämplig vid behandling av personuppgifter inom ramen för andra slags statistikprojekt, t.ex. vid framställning av verksamhetsstatistik. Sådan statistik, som alltså saknar samband med ett forskningsprojekt, torde inte komma att prövas av en forskningsetisk kommitté. Det saknas därför skäl att i dataskyddslagen införa en motsvarighet till 19 § tredje stycket PUL.

Svensk Försäkring menar att möjligheten att vidarebehandla uppgifter för statistikändamål bör vidgas och anför att försäkringsföretagen annars kommer att vara förhindrade att göra de aktuariella analyser som de är skyldiga att utföra för att uppfylla de näringsrättsliga kraven på god kontroll och uppföljning av verksamheten. Regeringen kan dock konstatera att den nu föreslagna bestämmelsen om behandling av känsliga personuppgifter för statistiska ändamål ger samma stöd för sådan behandling som bestämmelsen i 19 § andra stycket PUL. Det förtjänar också att poängteras att både artikel 6 och artikel 9.2 j i dataskyddsförordningen är direkt tillämpliga. De krav på lämpliga och särskilda åtgärder som ställs i artikel 9.2 j kan vara uppfyllda även genom andra bestämmelser än den föreslagna. Behandling av känsliga personuppgifter kan alltså ske med stöd av artikel 9.2 j även i andra fall, under förutsättning att lämpliga och särskilda åtgärder fastställts. Detta innebär t.ex. att en vidarebehandling av känsliga personuppgifter som samlats in av hänsyn till ett viktigt allmänt intresse, med stöd av gällande rätt som innehåller sådana lämpliga och särskilda åtgärder som krävs enligt artikel 9.2 g, får vidarebehandlas med direkt tillämpning av artikel 9.2 j i dataskyddsförordningen. Dataskyddsförordningen innebär således ingen ny begränsning i fråga om möjligheten att behandla känsliga personuppgifter för statistiska ändamål av viktigt allmänt intresse.

Användningsbegränsning

I avsnitt 14.1.4 angående behandling av personuppgifter för arkivändamål av allmänt intresse redogör regeringen för förslaget att dataskyddslagen ska innehålla en begränsning som motsvarar 9 § fjärde stycket PUL, när det gäller möjligheterna att vidta åtgärder i fråga om den registrerade. Regeringen anser, till skillnad från *dataskydd.net*, att en sådan användningsbegränsning utgör en väl avvägd skyddsåtgärd även i fråga om personuppgifter som behandlas för statistiska ändamål. Precis som i personuppgiftslagen bör bestämmelsen inte bara avse känsliga personuppgifter. Den nya bestämmelsen bör dock, som utredningen föreslår, utformas så att det tydligare än i dag framgår att användningsbegränsningen bara gäller personuppgifter som enbart behandlas för statistiska ändamål. Det är så bestämmelsen i personuppgiftslagen är avsedd att tillämpas och tillägget utgör därmed inte, som dataskydd.net anger, någon utvidgning av den personuppgiftsansvariges befogenheter.

Personuppgifter som enbart behandlas för statistiska ändamål bör därför få användas för att vidta åtgärder i fråga om den registrerade endast om det finns synnerliga skäl med hänsyn till den registrerades vitala intressen. Det saknas även här skäl att ange att uppgifter får användas med den registrerades samtycke. Begreppet vitala intressen bör tolkas och tillämpas likadant som enligt 9 § fjärde stycket PUL. Detta medför att det saknas skäl att, som *E-hälsomyndigheten* efterfrågar, utveckla förhållandet mellan begreppet vitala intressen och begreppet intressen som är av grundläggande betydelse.

Begränsningen i 9 § fjärde stycket PUL gäller inte vid myndigheters användning av uppgifter i allmänna handlingar (8 § andra stycket PUL). Undantaget motiveras i förarbetena med att det för sådana personuppgifter redan finns lämpliga skyddsåtgärder i form av bestämmelser om sekretess och skydd för arkiv. En allmän utgångspunkt för behandling av personuppgifter för statistiska ändamål är emellertid att resultatet eller uppgifterna inte används till stöd för åtgärder eller beslut som avser en särskild fysisk person (skäl 162). Enligt regeringens mening står det klart att det finns vissa undantagssituationer då uppgifter som annars bara behandlas för statistiska ändamål måste kunna användas även för att vidta sådana åtgärder, nämligen då den registrerades egna vitala intressen står på spel. I övrigt bör däremot inte heller myndigheter kunna använda uppgifterna för att vidta åtgärder i förhållande till den registrerade. Den omständigheten att uppgifterna finns i allmänna handlingar, eftersom dessa ännu inte hunnit anonymiseras eller gallras, föranleder ingen annan bedömning. Myndigheter bör därför inte undantas från den föreslagna användningsbegränsningen. Om det inom något verksamhetsområde eller för någon viss myndighet skulle finnas behov av ett sådant undantag bör det övervägas särskilt.

15 Sekretess

15.1 Sekretess hos tillsynsmyndigheten

Regeringens bedömning: Sekretess gäller enligt offentlighets- och sekretesslagen för skyddsvärda uppgifter i Datainspektionens tillsynsverksamhet. Någon förändring av de sekretessbestämmelser som är tillämpliga i Datainspektionens verksamhet behövs därför inte.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Det stora flertalet remissinstanser kommenterar inte utredningens bedömning i denna del. *Datainspektionen* anser att frågan om en sekretessbrytande reglering vid tillsynsmyndighetens internationella samarbete bör övervägas närmare. Vidare anser inspektionen, i likhet med bl.a. *Svensk Försäkring*, *Svenskt Näringsliv* och *IT&Telekomföretagen*, att absolut sekretess alternativt sekretess med omvänt skaderekvisit ska gälla i Datainspektionens verksamhet för anmälningar av personuppgiftsincidenter och för förhandssamråd. *Pensionsmyndigheten* är i och för sig av uppfattningen att det enligt gällande rätt finns goda möjligheter att skydda känslig information men anser att det är av vikt att frågan ägnas uppmärksamhet och analys under det fortsatta beredningsarbetet. *Migrationsverket* påpekar att det är av stor vikt att incidentrapporteringen realiseras på ett sådant sätt att den inte i sig bidrar till att negativt påverka den enskildes integritet, informationshanteringen i sig, it- och informationssäkerheten eller andra intressen med bäring på sekretess och säkerhetsskydd.

Skälen för regeringens bedömning: Enligt artikel 54.2 i dataskyddsförordningen ska varje tillsynsmyndighets ledamöter och personal, i enlighet med unionsrätten eller medlemsstaternas nationella rätt, omfattas av tystnadsplikt både under och efter sin mandattid vad avser konfidentiell information som de fått kunskap om under utförandet av deras uppgifter eller utövandet av deras befogenheter. Under mandatperioden ska tystnadsplikten i synnerhet gälla rapportering från fysiska personer om överträdelser av förordningen.

Som framgår av avsnitt 14.1.2 har regeringen för avsikt att, i förordning, peka ut Datainspektionen som tillsynsmyndighet enligt dataskyddsförordningen. Övervägandena kring tystnadsplikt för tillsynsmyndighetens ledamöter och personal sker med detta som utgångspunkt.

Hänvisningen i artikel 54.2 i dataskyddsförordningen till medlemsstaternas nationella rätt och begränsningen till konfidentiell information innebär att medlemsstaterna har relativt stort utrymme att utforma en lämplig reglering. I detta sammanhang finns det därför anledning att noga överväga om de sekretessbestämmelser som är tillämpliga i Datainspektionens verksamhet ger ett väl avvägt skydd för enskilda och allmänna intressen eller om någon av dem bör ändras.

Bestämmelser om sekretess i offentlighets- och sekretesslagen innebär både handlingssekretess och tystnadsplikt. En befattningshavare är skyldig att iaktta sekretess också sedan han eller hon har lämnat sin befattning. Det kan också noteras att tystnadsplikt enligt offentlighets- och sekretesslagen gäller även för företrädare för tillsynsmyndigheter i

andra medlemsstater som enligt artikel 62.3 i förordningen förordnats att utföra vissa uppgifter eller att inom ramen för vissa angivna befogenheter annars agera för den svenska tillsynsmyndighetens räkning, så länge kraven i 2 kap. 1 § OSL är uppfyllda.

Enligt 32 kap. 1 § OSL gäller sekretess hos Datainspektionen för uppgift om en enskilds personliga eller ekonomiska förhållanden, bl.a. i ärende om tillstånd eller tillsyn som enligt lag eller annan författning ska handläggas av inspektionen, om det kan antas att den enskilde eller någon närstående till denne lider skada eller men om uppgiften röjs.

Sekretessen tar alltså sikte på uppgifter som förekommer i Datainspektionens ärenden om tillstånd eller tillsyn. Det bör noteras att tillsynsbegreppet i offentlighets- och sekretesslagen är vitt. Således omfattar bestämmelsen exempelvis ärenden om personuppgiftsincidenter enligt artikel 33 och om förhandssamråd enligt artikel 36 i dataskyddsförordningen, eftersom EU-förordningar jämställs med lag. Om uppgifter har lämnats till Datainspektionen från en tillsynsmyndighet i någon annan medlemsstat inom ramen för det samarbete som förutsätts i förordningen sker detta på motsvarande sätt i ärende som omfattas av sekretessens räckvidd.

Sekretessens föremål enligt 32 kap. 1 § OSL är uppgifter om enskildas personliga eller ekonomiska förhållanden. Begreppet enskilda inbegriper förutom fysiska personer också företag, ideella föreningar och andra privaträttsliga juridiska personer. Det är därmed inte bara uppgifter om registrerade individer, t.ex. i ett kundregister eller i en myndighets ärendehanteringssystem, som skyddas av sekretessbestämmelsen. Den är tillämplig också i fråga om uppgifter som avslöjar den personuppgiftsansvariges företagshemligheter och andra affärs- eller driftförhållanden. Dessutom omfattar bestämmelsens föremål identiteten hos en fysisk person som har anmält missförhållanden till tillsynsmyndigheten.

Förutom 32 kap. 1 § OSL finns det flera andra sekretessbestämmelser som kan aktualiseras i Datainspektionens verksamhet. Exempelvis kan bestämmelserna om utrikessekretess i 15 kap. 1 § OSL och om sekretess i det internationella samarbetet i 15 kap. 1 a § OSL vara tillämpliga hos Datainspektionen i vissa situationer, liksom bestämmelsen i 15 kap. 2 § OSL till skydd för rikets säkerhet och försvar. Sekretess enligt 17 kap. 1 § OSL till skydd för inspektionsförberedelser kan också gälla i Datainspektionens tillsynsverksamhet. Samtliga dessa bestämmelser är, precis som flertalet sekretessbestämmelser i offentlighets- och sekretesslagen, försedda med raka skaderekvisit.

Enligt 18 kap. 8 § 3 OSL gäller sekretess bl.a. för uppgift som lämnar eller kan bidra till upplysning om säkerhetsåtgärd som avser system för automatiserad behandling av information, om det kan antas att syftet med åtgärden motverkas om uppgiften röjs. Denna bestämmelse är enligt sin ordalydelse tillämplig hos Datainspektionen både i fråga om säkerhetsåtgärder som redan har vidtagits av den personuppgiftsansvarige och rörande åtgärder som denne planerar. Vidare gäller den oavsett om den personuppgiftsansvarige är en myndighet eller ett privaträttsligt organ. Även denna bestämmelse är försedd med ett rakt skaderekvisit.

Datainspektionen har i en skrivelse till regeringen hemställt om att vissa sekretessfrågor ska utredas (Ju2017/06035/L6). I denna hemställan och i sitt yttrande över utredningens förslag anger Datainspektionen,

liksom flera andra remissinstanser, att sekretessen för uppgifter i bl.a. incidentrapporter inte är tillräcklig och att det krävs ett starkare sekretesskydd. *Föreningen Grävande journalister* och *Svenska journalistförbundet* invänder i särskilda skrivelser mot Datainspektionens hemställan.

Den omständigheten att samtliga ovan beskrivna sekretessbestämmelser är försedda med ett rakt skaderekvisit innebär inte, som Datainspektionen anför, att sekretesskyddet är svagt. Ett rakt skaderekvisit innebär visserligen att en presumtion för offentlighet gäller. Detta är också utgångspunkten för den svenska offentlighetsprincipen. Presumtionen för offentlighet bryts emellertid om det kan antas att en sådan skada som anges i sekretessbestämmelsen uppstår om uppgiften röjs. Enligt 32 kap. 1 § OSL gäller således sekretess om det kan antas att den enskilde eller någon närstående till denne lider skada eller men om uppgiften röjs. Enligt 15 kap. 1 § OSL gäller sekretess om det kan antas att det stör Sveriges mellanfolkliga förbindelser eller på annat sätt skadar landet om uppgiften röjs, medan det enligt 15 kap. 2 § OSL gäller sekretess om det kan antas att det skadar landets försvar eller på annat sätt vållar fara för rikets säkerhet om uppgiften röjs. Enligt 18 kap. 8 § 3 OSL gäller slutligen sekretess om det kan antas att syftet med säkerhetsåtgärden motverkas om uppgiften röjs.

Om det vid tillämpningen av någon av dessa bestämmelser kan antas att ett röjande skulle leda till den angivna skadan är uppgiften sekretessbelagd och därmed hemlig. Uppgiften får då inte utan särskilt lagstöd lämnas ut och inte heller röjas muntligen. Detta röjandeförbud gäller dessutom oavsett om uppgiften förekommer i en allmän handling eller inte.

Ett rakt skaderekvisit innebär normalt att det är uppgifternas karaktär som får avgöra om sekretess gäller eller inte. Om uppgiften är sådan att den genomsnittligt sett måste betraktas som harmlös ska den alltså normalt anses vara offentlig. Om uppgiften i stället typiskt sett måste betraktas som känslig omfattas den normalt av sekretess. Skaderekvisitet kan alltså uppfattas som en metod att precisera föremålet för sekretessen eller dess räckvidd (prop. 1979/80:2 Del A s. 77–78).

Bestämmelsen i 18 kap. 8 § 3 OSL har i ett tidigare lagstiftningsärende ansetts innebära att uppgifter om ingivare av incidentrapportering avseende säkerhetsbrister i it-system till Post- och telestyrelsen, liksom uppgifter om innehållet i rapporterna, omfattas av sekretess (prop. 2003/04:93 s. 82). Utredningen om genomförande av NIS-direktivet har dessutom nyligen utrett om bestämmelsen behöver ändras för att känslig information i incidentrapporter som lämnas till Myndigheten för samhällsskydd och beredskap ska kunna skyddas. Den utredningen konstaterar i sitt betänkande att 18 kap. 8 § OSL ger ett tillräckligt skydd för uppgifter som kan komma att rapporteras vid en incident (SOU 2017:36 s. 247–257).

Regeringen kan konstatera att såväl incidentrapporter som anmälningar om förhandssamråd, liksom andra handlingar hos Datainspektionen, kan innehålla skyddsvärd information rörande enskildas ekonomiska förhållanden av det slag för vilka sekretess gäller enligt 32 kap. 1 § OSL. Handlingarna kan även innehålla sådan skyddsvärd information rörande säkerhetsåtgärder som avses i 18 kap. 8 § 3 OSL. Det senare gäller oavsett om ingivaren är en myndighet eller ett privaträttsligt organ.

Som utredningen påpekar kan den incidentrapportering som förutsätts ske till tillsynsmyndigheten i enlighet med artikel 33 i förordningen i praktiken innebära en upplysning om att ingivarens it-system är sårbart för attacker. Uppgiften om vem som har lämnat in en sådan rapport utgör alltså i sig en uppgift som kan omfattas av sekretessens föremål enligt 18 kap. 8 § 3 OSL, eftersom den lämnar upplysning om att ingivarens säkerhetsåtgärder har brister. I många fall kan det antas att den personuppgiftsansvariges säkerhetsåtgärder motverkas om det framkommer att dessa har brister. Bestämmelsens skaderekvisit är i sådana situationer uppfyllt, varvid sekretess gäller. Ett utlämnande av uppgifter som avslöjar vid vilka tillfällen en viss personuppgiftsansvarig har lämnat incidentrapporter kan på motsvarande sätt utgöra en säkerhetsrisk, med tanke på att uppgifterna skulle kunna användas för kartläggning av den personuppgiftsansvariges förmåga att upptäcka intrång. Uppgiften om ingivarens identitet bör därmed typiskt sett anses vara känslig, i vart fall under den närmaste tiden efter att incidentrapportering skett.

Konstruktionen med ett rakt skaderekvisit tillgodoser allmänhetens berättigade intresse av insyn i tillsynsmyndighetens verksamhet, eftersom harmlösa uppgifter får lämnas ut. Samtidigt tillgodoser de aktuella sekretessbestämmelserna de registrerades och de personuppgiftsansvarigas berättigade intresse av diskretion, eftersom uppgifter inte får röjas om det kan antas leda till skada. Regeringen anser mot denna bakgrund att den befintliga sekretessregleringen ger ett väl avvägt skydd för såväl enskilda som allmänna intressen. Bestämmelserna i offentlighets- och sekretesslagen, som vid behov bör tolkas unionskonformt (jfr prop. 1997/98:44 s. 146), uppfyller också kraven på skydd för konfidentiell information i dataskyddsförordningen. Någon ändring av den sekretessreglering som gäller i Datainspektionens verksamhet är därmed inte nödvändig för att Sverige ska uppfylla sina unionsrättsliga skyldigheter. Regeringen anser inte heller att det framkommit några omständigheter som medför att en sådan ändring bör ske av andra skäl. Regeringen ser därför för närvarande inte skäl att, som Datainspektionen hemställt, utreda sekretessfrågan ytterligare.

Vidare anför *Datainspektionen* att frågan om en sekretessbrytande reglering vid tillsynsmyndighetens internationella samarbete bör övervägas närmare. Av 8 kap. 3 § OSL framgår emellertid att en uppgift för vilken sekretess gäller får röjas för en utländsk myndighet eller en mellanfolklig organisation, om utlämnande sker i enlighet med särskild föreskrift i lag eller förordning. EU-förordningar jämställs med lag vid tillämpningen av offentlighets- och sekretesslagen. Sekretess utgör således inget hinder för det informationsutbyte som enligt artikel 57.1 g i dataskyddsförordningen ska ske mellan tillsynsmyndigheterna. Regeringen ser mot denna bakgrund inte skäl att göra några ytterligare överväganden i denna del.

15.2 Tystnadsplikt för dataskyddsombud

Regeringens förslag: Den som fullgör uppgift som dataskyddsombud enligt EU:s dataskyddsförordning får inte obehörigen röja det som han eller hon vid fullgörandet av sin uppgift har fått kännedom om. I det allmännas verksamhet ska i stället offentlighets- och sekretesslagen tillämpas.

Utredningens förslag överensstämmer delvis med regeringens. Enligt utredningens förslag ska tystnadsplikten gälla det som den som utsetts till dataskyddsombud har fått veta om enskilds personliga eller ekonomiska förhållanden.

Remissinstanserna: Majoriteten av remissinstanserna tillstyrker utredningens förslag eller har inga synpunkter på det. *Malmö kommun* och *Piteå kommun* konstaterar att förslaget inte innebär någon förändring i sekretesshänseende i förhållande till vad som gäller i dag för ett av kommunen anställt personuppgiftsombud. *Förvaltningsrätten i Malmö* ställer sig dock tveksam till bedömningen att offentlighets- och sekretesslagens nuvarande bestämmelser uppfyller dataskyddsförordningens krav på tystnadsplikt för dataskyddsombud i det allmännas verksamhet samt anser att frågan bör analyseras ytterligare. *Pensionsmyndigheten*, *Statens servicecenter*, *Lantmäteriet* och *Sveriges advokatsamfund* anser att utredningens förslag inte är tillräckliga för att uppfylla förordningens krav på tystnadsplikt för dataskyddsombud inom offentlig verksamhet. *Jordbruksverket* anför att det bör övervägas ett tydliggörande av sekretessregleringen avseende de sammanställningar av uppgifter som kan komma att uppstå i dataskyddsombudets verksamhet och av uppgifter som kommer att uppstå vid sammanställning för att förse den registrerade med kopia av de personuppgifter som är under behandling. *Forum för dataskydd* anser att det skulle vara tydligare och enklare att reglera dataskyddsombudets tystnadsplikt i dataskyddslagen för den privata sektorn och införa en likalydande bestämmelse i offentlighets- och sekretesslagen. Det bör enligt Forum för dataskydd tydligt framgå att dessa bestämmelser inte bara avser enskildas personliga och ekonomiska förhållanden, utan även personuppgiftsansvarigas och personuppgiftsbiträdens förhållanden. *Umeå universitet* anser, i fråga om den föreslagna bestämmelsen om tystnadsplikt för dataskyddsombud, att starka skäl talar för att bestämmelsen bör konstrueras på ett mer förutsägbart sätt. Universitetet förordar att det direkt av lagtexten bör framgå att det inte är fråga om ett obehörigt röjande om den som uppgiften rör samtycker till ett utlämnande eller om utlämnandet följer av en skyldighet i lag eller förordning. Vidare bör det enligt universitetet framgå om uppgiftsskyldighet i lag eller förordning bryter tystnadsplikten i förhållande till såväl myndigheter som enskilda eller endast i förhållande till antingen myndigheter eller enskilda. *Svensk Försäkring* anser att frågan om vad som är ett behörigt utlämnade bör belysas ytterligare, inte minst eftersom tystnadsplikten föreslås bli straffbelagd. *Svenskt Näringsliv* tillstyrker förslaget om tystnadsplikt för dataskyddsombud men förordar en annan utformning av bestämmelsen, likt den som gäller för revisorer. Även *Näringslivets regelnämnd* invänder mot den föreslagna formuleringen och anser att den skulle kunna innebära att företagshemligheter röjs.

Sveriges Television AB anser att dataskyddsombudets tystnadsplikt även bör omfatta information som avser den personuppgiftsansvariges eller personuppgiftsbiträdets säkerhetsåtgärder och driftsförhållanden. *Sveriges advokatsamfund* anser att tystnadsplikten bör omfatta alla uppgifter som dataskyddsombudet erhåller i denna sin roll och inte endast uppgifter om enskilds personliga och ekonomiska förhållanden.

Skälen för regeringens bedömning

Regleringen i förordningen

Ett dataskyddsombud ska enligt artikel 39 i dataskyddsförordningen ha till uppgift att informera personuppgiftsansvariga, personuppgiftsbiträden och anställda om skyldigheterna enligt förordningen och andra dataskyddsbestämmelser. Ombudet ska också bl.a. övervaka efterlevnaden av förordningen och samarbeta med tillsynsmyndigheten.

Enligt artikel 37.1 i dataskyddsförordningen måste myndigheter och offentliga organ som behandlar personuppgifter utnämna dataskyddsombud. Detsamma gäller personuppgiftsansvariga eller personuppgiftsbiträden som utför behandling där omfattningen, ändamålen eller uppgifternas karaktär motiverar att ett ombud utses. I artiklarna 37.5 och 38 finns bestämmelser om dataskyddsombudets kvalifikationer och ställning. I artikel 37.6 stadgas att dataskyddsombudet får ingå i den personuppgiftsansvariges eller personuppgiftsbiträdets personal eller utföra uppgifterna på grundval av ett tjänsteavtal. Flera myndigheter eller flera bolag i en koncern kan ha ett gemensamt dataskyddsombud under vissa förutsättningar (artikel 37.2–3).

Enligt artikel 38.5 ska dataskyddsombudet, när det gäller dennes genomförande av sina uppgifter, vara bundet av sekretess eller konfidentialitet i enlighet med unionsrätten eller medlemsstaternas nationella rätt. Det finns inget uttalande i skälen till dataskyddsförordningen som ger vägledning vid tolkning av denna bestämmelse. Det faktum att bestämmelsen hänvisar till nationell rätt innebär dock att medlemsstaterna har stor frihet att utforma en lämplig reglering.

Dataskyddsombud i offentlig sektor

I det allmännas verksamhet gäller sekretess för vissa uppgifter enligt offentlighets- och sekretesslagen. Regleringen är detaljerad och differentierad och har anpassats med hänsyn till uppgifternas känslighet, intresset av insyn och intresset av skydd i vissa specifika verksamheter. Det är förbjudet för myndigheter att röja en sekretessbelagd uppgift. Förbudet gäller också för en person som fått kännedom om uppgiften genom att för det allmännas räkning delta i en myndighets verksamhet på grund av anställning eller uppdrag hos myndigheten, på grund av tjänsteplikt eller på annan liknande grund (2 kap. 1 § OSL).

Regeringen bedömer, liksom *Förvaltningsrätten i Malmö*, att ett dataskyddsombud inte kan anses uppträda självständigt i förhållande till den övriga verksamheten inom myndigheten i den mening som avses i 2 kap. 8 § TF. På många sätt påminner dataskyddsombudets ställning om den som en internrevisor intar när det gäller självständighet och förhållande till ledningen. Högsta förvaltningsdomstolen har i HFD 2013 ref. 40

bedömt att en internrevisor vid Jordbruksverket inte intog en sådan självständig ställning att en rapport som överlämnats till den granskade verksamheten skulle anses expedierad.

För det allmännas räkning kan det enligt utredningens mening inte komma ifråga att särskilt reglera sekretessen för dataskyddsombud, utöver den sekretess som redan gäller i alla de vitt skilda verksamhetstyper som omfattas av dataskyddsförordningens tillämpningsområde. Det får enligt utredningens bedömning förutsättas att det i verksamheter där känsliga uppgifter förekommer redan gäller sekretess enligt offentlighets- och sekretesslagen i den utsträckning som är motiverad i just den verksamheten. Så länge dataskyddsombudet innehar en sådan anställning eller uppdrag som avses i 2 kap. 1 § andra stycket OSL omfattas han eller hon av sekretessen. Utredningens bedömning är att ett dataskyddsombud i allmänhet får anses delta i verksamheten på ett sådant sätt som förutsätts i nämnda bestämmelse.

Förvaltningsrätten i Malmö anser att denna fråga bör analyseras ytterligare. Bland annat anser förvaltningsrätten att dataskyddsombudets uppgifter knappast kan anses vara en del av den personalsociala eller personaladministrativa verksamheten och att ombudet därmed inte skulle kunna omfattas av tystnadsplikt enligt 39 kap. OSL. Liknande invändningar framförs av bl.a. *Pensionsmyndigheten*.

Regeringen vill dock understryka att skyddet av personuppgifter utgör en integrerad del av all verksamhet där behandling av personuppgifter förekommer. Dataskyddsombudets befattning med personuppgifter är därmed direkt kopplad till den personuppgiftsansvariges verksamhet. Regeringen instämmer i utredningens uppfattning att ett dataskyddsombud måste anses delta i myndighetens verksamhet på det sätt som avses i 2 kap. 1 § OSL. Dataskyddsombudet omfattas därmed av offentlighets- och sekretesslagens förbud att röja eller utnyttja de sekretessbelagda uppgifter som ombudet får kännedom om. Detta gäller oavsett om uppgiften förekommer i ett ärende, i personaladministrativ verksamhet eller i någon annan del av myndighetens verksamhet där sekretess gäller för uppgiften.

Som *Malmö kommun* och *Piteå kommun* konstaterar innebär denna bedömning inte någon förändring i förhållande till vad som gäller i dag för ett personuppgiftsombud i offentlig sektor. På motsvarande sätt förändras inte heller synsättet på sådana sammanställningar som skapas enbart för att tillgodose den registrerades rätt till s.k. registerutdrag. Någon sådan förändring är inte heller motiverad med anledning av artikel 38.5 i dataskyddsförordningen, eftersom den bestämmelsen, som nämns ovan, ger medlemsstaterna stor frihet att utforma en lämplig reglering. Mot denna bakgrund anser regeringen att det [hittills] inte framkommit skäl att ytterligare utreda frågan om tystnadsplikt för dataskyddsombud i det allmännas verksamhet.

Personuppgiftsombud i privat sektor

Offentlighets- och sekretesslagen är, med vissa undantag, inte tillämplig utanför den offentliga sektorn. För att Sverige ska uppfylla dataskyddsförordningens krav måste därför bestämmelser om tystnadsplikt för dataskyddsombud i den privata sektorn införas.

I den privata sektorn gäller som huvudregel att den som disponerar över information själv bestämmer om utlämnande av den till andra, med de begränsningar som dataskyddsregleringen ställer upp. Inom flera olika verksamhetsområden i den privata sektorn gäller emellertid tystnadsplikt enligt lag, ofta reglerad som ett förbud mot att röja vissa uppgifter obehörigen. Det gäller bl.a. verksamheter i välfärdssektorn, t.ex. enskilt bedriven förskola (29 kap. 14 § skollagen) och hälso- och sjukvård (6 kap. 12 § patientsäkerhetslagen). Men det finns också tystnadsplikter i privat verksamhet som inte har någon motsvarighet i det allmännas verksamhet, utan skyddar information som lämnas till personer i olika slag av förtroendeställning, exempelvis tystnadsplikt för revisorer (26 § revisorslagen [2001:883]) och skyddsombud (7 kap. 13 § arbetsmiljölagen), eller den tystnadsplikt som följer av den så kallade banksekretessen (bl.a. 1 kap. 10 § lagen [2004:297] om bank- och finansieringsrörelse).

I dessa fall har obehörighetsrekvisitet sammanfattningsvis tolkats som att ett utlämnande av uppgifter får ske bl.a. om den som uppgiften rör har lämnat sitt samtycke, om uppgifter lämnas vidare till personer inom den berörda verksamheten som behöver dem för verksamheten eller om uppgifterna enligt lag eller annan författning ska lämnas ut, exempelvis till en tillsynsmyndighet (se t.ex. prop. 2002/03:139 s. 479).

Författningsreglerad tystnadsplikt, oavsett om den följer av offentlighets- och sekretesslagen eller av bestämmelser om tystnadsplikt för den privata sektorn, är som regel förenad med straffansvar. I 20 kap. 3 § brottsbalken regleras det generella straffansvaret för brott mot tystnadsplikt. Straffansvaret gäller var och en som har skyldighet att hemlighålla en uppgift enligt lag eller annan författning, förutsatt att straffansvaret inte har reglerats särskilt. Konsekvensen av att en tystnadsplikt införs i författning blir alltså, om inget annat stadgas, att det med regleringen följer ett straffansvar.

Som framgår ovan finns det en rad tystnadsplikter för personer som, i egenskap av sin ställning och för att kunna utföra sitt uppdrag, måste åtnjuta förtroende, t.ex. revisorer och skyddsombud. Dataskyddsombudets ställning kan i vissa avseenden likställas med revisorns eller skyddsombudets, och tystnadsplikten för dataskyddsombud bör därför utformas på ett liknande sätt.

Utredningens förslag innebär att den som utsetts till dataskyddsombud inte obehörigen får röja det som han eller hon vid fullgörandet av sin uppgift har fått veta om enskilds personliga och ekonomiska förhållanden. Några remissinstanser, bl.a. *Svenskt Näringsliv* och *Sveriges Television AB*, invänder mot den föreslagna formuleringen och påpekar att tystnadsplikten bör omfatta information som avser den personuppgiftsansvariges eller personuppgiftsbiträdets säkerhetsåtgärder och driftsförhållanden. Med begreppet enskild avses emellertid både fysiska och juridiska personer. Således omfattas t.ex. ett företags drifts- och affärsförhållanden av den föreslagna formuleringen. Som *Sveriges advokatsamfund* påpekar kan dock avgränsningen till personliga och ekonomiska förhållanden leda till svåra avvägningar i fråga om vad som omfattas av dataskyddsombudets tystnadsplikt. Någon sådan avgränsning finns inte i motsvarande bestämmelser om tystnadsplikt för advokater eller revisorer. Det framgår inte heller klart av dataskyddsförordningen

att det endast är uppgifter om personliga och ekonomiska förhållanden som ska skyddas. Det är vidare, som *Forum för dataskydd* framhåller, angeläget att personuppgiftsansvariga och personuppgiftsbiträden vågar lämna all den information som dataskyddsombudet behöver för att fullgöra sina uppgifter. Med beaktande av att det inom den privata sektorn inte finns något motstående insynsintresse, anser regeringen därför att den av utredningen föreslagna avgränsningen till enskildas personliga och ekonomiska förhållanden bör tas bort. Tystnadsplikten bör i stället gälla för alla slags uppgifter som dataskyddsombudet vid fullgörandet av sin uppgift har fått kännedom om.

Svensk Försäkring anser att frågan om vad som är ett behörigt utlämnande bör belysas ytterligare, inte minst eftersom tystnadsplikten föreslås bli straffbelagd. Vidare anser *Umeå universitet* att det direkt av lagtexten bör framgå i vilka fall det inte är fråga om ett obehörigt röjande. Enligt regeringens mening är det dock inte lämpligt att uttömmande reglera i vilka fall utlämnande får ske. Detta måste bedömas utifrån omständigheterna i det enskilda fallet. Uppgifter kan dock normalt lämnas ut med samtycke från den uppgiften avser, till tillsynsmyndigheten eller annars som en följd av en skyldighet i lag eller författning.

Det finns i svensk rätt, som nämns ovan, flera bestämmelser om tystnadsplikt där obehörighetsrekvisitet används. Den praxis som finns rörande dessa bestämmelser bör i fråga om rekvisitets innebörd kunna tjäna som ledning även vid tolkningen och tillämpningen av den nu föreslagna bestämmelsen. Regeringen anser således att bestämmelsen bör ange att den som fullgör uppgift som dataskyddsombud inte får obehörigen röja det som han eller hon vid fullgörandet av sin uppgift har fått kännedom om.

15.3 Sekretess för uppgifter som behandlas i strid med personuppgiftsregleringen

Regeringens förslag: Sekretess gäller för personuppgift, om det kan antas att uppgiften efter ett utlämnande kommer att behandlas i strid med EU:s dataskyddsförordning, i den ursprungliga lydelsen, eller dataskyddslagen.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Det stora flertalet remissinstanser tillstyrker förslaget eller har inga synpunkter på det. *Domstolsverket* påpekar att bestämmelsen, såsom den är utformad, inte torde omfatta bestämmelser i den till dataskyddslagen anslutande förordningen. *Centrala studiestödsnämnden*, som instämmer i utredningens förslag, anser att hänvisningen till förordningen i statisk lydelse kan medföra vissa lagtekniska svårigheter vid ändringar i förordningen, vilket sammantaget riskerar att göra tillämpningen av bestämmelsen mer oöverskådlig. *Arbetsförmedlingen* anser att det i bestämmelsen bör införas en hänvisning även till forskningsdatalagen. *Svenska journalistförbundet* och *Tjänstemännens centralorganisation* anser att regeln på sikt bör upphävas och kan därför inte tillstyrka förslaget.

Skälen för regeringens förslag: Enligt 21 kap. 7 § OSL gäller sekretess för personuppgifter, om det kan antas att ett utlämnande skulle medföra att uppgiften behandlas i strid med personuppgiftslagen. Det får numera anses fastslaget i praxis att bestämmelsen enbart tar sikte på mottagarens behandling av personuppgifter (HFD 2014 ref. 66). Det som ska bedömas enligt bestämmelsen är alltså endast huruvida mottagarens avsedda behandling av de personuppgifter som begärs ut uppfyller kraven enligt personuppgiftslagen.

Bestämmelsen i 21 kap. 7 § OSL har utretts flera gånger under 2000-talet, men inga förslag till ändringar har genomförts. Eftersom personuppgiftslagen nu ska upphävas och den generella dataskyddsregleringen i stället kommer att finnas i dataskyddsförordningen och den nya dataskyddslagen, måste dock bestämmelsen ändras. Det finns däremot inte skäl att, som *Svenska journalistförbundet* och *Tjänstemännens centralorganisation* föreslår, upphäva sekretessbestämmelsen.

Utredningen föreslår att hänvisningen till personuppgiftslagen ska ersättas med en hänvisning till dataskyddsförordningen och dataskyddslagen. Detta kan, som utredningen påpekar, innebära en risk för att den prövning som ska utföras kompliceras något. Förordningens bestämmelser är betydligt mer omfattande och i vissa avseenden mer detaljerade än personuppgiftslagens. Det bör dock betonas att det som en utlämnande myndighet ska pröva är om det kan antas att en uppgift efter ett utlämnande kommer att behandlas i strid med förordningen eller dataskyddslagen. Som framgår av Riksdagens ombudsmäns uttalanden (dnr 1102-2004) får vidare undersökningar vidtas endast om det finns konkreta omständigheter som indikerar att mottagaren kommer att behandla uppgifterna på ett sätt som strider mot dataskyddsregleringen, t.ex. massuttag eller selekterade uttag. Finns det inga sådana indikationer behöver inte någon bedömning enligt dataskyddsregleringen göras. Rekvisitet kan antas torde också innebära att någon fullständig bedömning av om behandlingen kommer att strida mot förordningen inte krävs.

Som *Domstolsverket* och *Arbetsförmedlingen* påpekar kommer det i svensk rätt att finnas andra författningar än dataskyddslagen som innehåller bestämmelser om behandling av personuppgifter. Detta skiljer sig dock inte från hur regelverket är utformat i dag, där personuppgiftslagen kompletteras av en rad andra författningar, bl.a. personuppgiftsförordningen. Bestämmelsen i 21 kap. 7 § OSL hänvisar dock endast till personuppgiftslagen. Utredningen föreslår inte att sekretessbestämmelsens tillämpningsområde ska utsträckas till att även omfatta t.ex. behandling av utlämnade uppgifter som kan antas strida mot registerförfattningar. Konsekvenserna av en sådan utvidgning är således inte heller utredda. Regeringen lämnar därför inte något sådant förslag.

Sekretess enligt 21 kap. 7 § OSL gäller inte om de utlämnade uppgifterna ska behandlas av personuppgiftsansvariga som är etablerade utomlands, där personuppgiftslagen inte är tillämplig (HFD 2014 ref. 66). Förslaget medför emellertid att utlämnanden till utländska mottagare som omfattas av dataskyddsförordningens tillämpningsområde också kommer att omfattas av sekretessbestämmelsen. Regeringen anser, i likhet med utredningen, att denna materiella utvidgning av bestämmelsens tillämpningsområde är rimlig och ligger väl i linje med de grundläggande principerna i dataskyddsförordningen.

Eftersom det numera är klarlagt att prövningen av 21 kap. 7 § OSL gäller den behandling som kommer att ske efter ett eventuellt utlämnande bör lagtexten justeras på det sätt utredningen föreslår så att det tydligt framgår att det är behandling efter ett utlämnande som avses.

Eftersom hänvisningen till dataskyddsförordningen avser förordningen i dess helhet och innebär en inskränkning i den grundlagsstadgade handlingsoffentligheten bör hänvisningen vara statisk, dvs. avse den ursprungliga lydelsen av förordningen. Det medför att lagstiftaren aktivt måste bedöma om eventuella ändringar och tillägg till förordningen ska omfattas av 21 kap. 7 § OSL. Mot bakgrund av att förordningen sannolikt inte kommer att ändras särskilt ofta, delar regeringen inte *Centrala studiestödsnämndens* farhågor om att den statiska hänvisningen riskerar att göra tillämpningen av bestämmelsen mer oöverskådlig.

Sammanfattningsvis anser regeringen att 21 kap. 7 § OSL bör ändras i enlighet med utredningens förslag, så att sekretess gäller för personuppgift, om det kan antas att uppgiften efter ett utlämnande kommer att behandlas i strid med dataskyddsförordningen, i den ursprungliga lydelsen, eller dataskyddslagen.

15.4 Generalklausulen

Regeringens förslag: Hänvisningen till personuppgiftslagen i den s.k. generalklausulen i offentlighets- och sekretesslagen tas bort. Generalklausulen ska enligt den nya lydelsen inte gälla om utlämnandet strider mot lag eller förordning.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna tillstyrker förslaget eller har inga synpunkter på det.

Skälen för regeringens förslag: Enligt den s.k. generalklausulen i 10 kap. 27 § OSL 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. Bestämmelsen möjliggör informationsutbyte mellan myndigheter av uppgifter som omfattas av sekretess i fall då det saknas uttryckliga sekretessbrytande regler. Utlämnandet ska då prövas enligt den intresseavvägning och med beaktande av det uppenbarhetsrekvisit som framgår av bestämmelsen. Av paragrafens andra stycke framgår att uppgifter som omfattas av viss sekretess, som hälso- och sjukvårdssekretessen och socialtjänstsekretessen, inte kan lämnas ut med stöd av generalklausulen.

I tredje stycket samma paragraf undantas också utlämnanden som strider mot lag eller förordning eller föreskrift som har meddelats med stöd av personuppgiftslagen från tillämpningsområdet. Första ledet har ansetts innebära att en förutsättning för att generalklausulen ska vara tillämplig är att utlämnandet inte strider mot en sådan specialreglering av uppgiftslämnandet som finns i lag eller förordning. Om det t.ex. i lag har föreskrivits att en viss myndighet för sin verksamhet på angivna villkor kan få ta del av även hemliga uppgifter hos en annan myndighet, kommer det inte i fråga att, när de angivna villkoren inte är uppfyllda, lämna ut

uppgifterna med stöd av generalklausulen i stället (prop. 1979/80:2, del A s. 328).

Innebörden av tredje styckets andra led är numera oklar. Tidigare avsåg den en möjlighet för Datainspektionen att meddela vissa villkor om utlämnande för vissa register i samband med tillståndsgivning. Utredningen konstaterar dock att bestämmelsen inte längre tycks fylla någon praktisk funktion.

Det första ledet i generalklausulens tredje stycke innebär enligt sin ordalydelse att ett utlämnande till annan myndighet med stöd av generalklausulen inte får ske om det skulle strida mot lag eller förordning, exempelvis mot personuppgiftslagen. En hänvisning till lag i offentlighets- och sekretesslagen innefattar också EU-förordningar. Redan det första ledet torde alltså innebära att ett utlämnande till en annan myndighet som strider mot dataskyddsförordningen eller dataskyddslagen inte kan ske med stöd av generalklausulen. Någon motsvarighet till andra ledet i tredje stycket behövs inte som en följd av den nya regleringen och bör därför tas bort.

16 Sanktioner

16.1 Sanktionsavgifter enligt dataskyddsförordningen

Administrativa sanktionsavgifter är en nyhet i dataskyddsförordningen som saknar motsvarighet i dataskyddsdirektivet och personuppgiftslagen. Sanktionsavgifterna införs enligt skäl 148 för att stärka verkställigheten av förordningen.

Bestämmelserna om administrativa sanktionsavgifter återfinns i förordningens artikel 83 och förtydligas i skäl 148–150. Bestämmelserna är direkt tillämpliga i förhållande till privaträttsliga organ och ger inget utrymme för medlemsstaterna att specificera bestämmelserna eller att föreskriva några undantag i förhållande till sådana organ. Av artikel 83.1 framgår att det är den nationella tillsynsmyndigheten som ska besluta om sanktionsavgifter vid överträdelser av förordningens bestämmelser. I artikel 83.2 anges vilka faktorer som ska beaktas vid beslut om sanktionsavgifter och bestämmande av avgiftens storlek. Tillsynsmyndigheten ska vid beslutet bl.a. beakta överträdelsens karaktär, svårighetsgrad och varaktighet, samt om överträdelsen skett med uppsåt eller genom oaktsamhet. Andra faktorer som tillsynsmyndigheten ska beakta är bl.a. antalet berörda registrerade, vilken skada de har lidit, om den personuppgiftsansvarige har försökt förebygga eller i efterhand komma till rätta med överträdelsen och eventuell ekonomisk vinst som görs, eller ekonomisk förlust som undviks, genom överträdelsen.

I artikel 83.3 stadgas att om flera överträdelser sker får avgiftens totala belopp inte överstiga det belopp som fastställs för den allvarligaste överträdelsen. I artikel 83.4 och 83.5 fastställs övre beloppsgränser för de två olika kategorier av överträdelser som kan föranleda sanktionsavgifter enligt förordningen. För de något mindre allvarliga överträdelserna,

såsom överträdelser av regler om inbyggt dataskydd, förteckningar och konsekvensbeskrivningar, fastslås ett maxbelopp på 10 000 000 EUR eller 2 procent av den globala årsomsättningen om det gäller ett företag, beroende på vilket belopp som är högst. För allvarligare överträdelser, såsom överträdelser av reglerna om de grundläggande principerna för behandling, registrerades rätt till information, rättelse och radering, överföring av uppgifter till tredjeland och underlåtenhet att rätta sig efter tillsynsmyndighetens förelägganden, fastslås ett maxbelopp om 20 000 000 EUR eller 4 procent av den globala årsomsättningen, beroende på vilket belopp som är högst.

Det stora flertalet bestämmelser i förordningen som innehåller rättigheter för registrerade eller skyldigheter för personuppgiftsansvariga, personuppgiftsbiträden, certifieringsorgan och övervakningsorgan omfattas av regleringen om sanktionsavgifter, vilket framgår av artikel 83.4–6. Artikel 10, om behandling av personuppgifter som rör lagöverträdelser, nämns dock inte i artikel 83.4–6. Sanktionsavgifter kan alltså enligt förordningen inte påföras vid överträdelser av artikel 10.

Bestämmelserna om sanktionsavgifter innehåller inte enbart en uppräkning av de överträdelser som i sig kan föranleda att sanktionsavgift påförs. De föreskriver också att sanktionsavgifter kan påföras vid underlåtelse att rätta sig efter tillsynsmyndighetens förelägganden eller beslut. En avgift kan då påföras med det högre maxbeloppet, dvs. 20 000 000 EUR eller 4 procent av den globala årsomsättningen, beroende på vilket belopp som är högst (artikel 83.5 e och 83.6). Sanktionsavgiften fyller i dessa fall en vitesliknande funktion.

16.2 Sanktionsavgifter inom offentlig sektor

Regeringens förslag: Tillsynsmyndigheten får ta ut sanktionsavgifter även av statliga och kommunala myndigheter vid överträdelser av bestämmelserna i EU:s dataskyddsförordning. För mindre allvarliga överträdelser ska avgiften uppgå till högst 5 000 000 kronor och för allvarligare överträdelser till högst 10 000 000 kronor. Vid bestämmandet av avgiftens storlek i det enskilda fallet ska dataskyddsförordningens bestämmelser tillämpas.

Utredningens förslag överensstämmer delvis med regeringens. Utredningen föreslår högre maxbelopp. Vidare föreslår utredningen att bestämmelsens hänvisning till dataskyddsförordningen ska vara dynamisk, se avsnitt 5.1.2. Utredningens förslag har även en delvis annan utformning.

Remissinstanserna: En majoritet av remissinstanserna tillstyrker utredningens förslag eller har inga synpunkter på det. Ett antal instanser, bl.a. *Polismyndigheten*, *Försäkringskassan* och *Myndigheten för vård- och omsorgsanalys*, avstyrker förslaget i dess helhet. Några av de instanser som instämmer i att sanktionsavgifter ska kunna tas ut av myndigheter, bl.a. *Företagarna* och *Stiftelsen för internetinfrastruktur*, anser att avgiften ska uppgå till lika höga maxbelopp som för enskilda. Andra remissinstanser som instämmer i utredningens bedömning i denna del, t.ex. *Centrala studiestödsnämnden*, *Göteborgs universitet*, *Trafikverket* och *Sveriges Kommuner och Landsting*, anser att maxbeloppet

tvärtom bör vara lägre än vad utredningen föreslår. Vidare menar några remissinstanser, bl.a. *Skolverket*, *Falköpings kommun* och *Östergötlands läns landsting*, att beloppet bör vara beroende av myndighetens storlek eller budgetram. Falköpings kommun och *Jönköpings läns landsting* anser att det behöver klargöras om kommunala bolag omfattas av förslaget.

Skälen för regeringens förslag: Enligt artikel 83.7 är det upp till varje medlemsstat att fastställa regler om och i vilken utsträckning sanktionsavgifter ska kunna påföras offentliga myndigheter och organ i den medlemsstaten. Utredningen föreslår att svenska myndigheter ska kunna påföras sanktionsavgifter vid överträdelser av dataskyddsregleringen, dock med lägre högsta belopp än de som enligt dataskyddsförordningen gäller för privata aktörer.

Enligt regeringsformens terminologi, som bör användas även vid tolkningen av dataskyddsförordningen (se avsnitt 8.1), är alla offentliga organ utom riksdagen och kommun- och landstingsfullmäktige myndigheter. Privaträttsliga organ är varken myndigheter eller offentliga organ, även om de utövar offentlig makt. Med anledning av *Falköpings kommuns* och *Jönköpings läns landstings* synpunkt kan det således konstateras att kommunala bolag bör anses som privata organ vid tillämpningen av dataskyddsförordningen och att de därmed inte omfattas av utredningens förslag. Däremot omfattas de av de direkt tillämpliga bestämmelserna om sanktionsavgifter i dataskyddsförordningen.

Flera av de remissinstanser som är kritiska till utredningens förslag om att sanktionsavgifter ska kunna tas ut av myndigheter ifrågasätter sanktionsavgifternas effektivitet, främst i förhållande till statliga myndigheter. Till exempel menar *Göteborgs universitet* att betalningen av en hög avgift minskar utrymmet för myndigheten att fullgöra sitt egentliga uppdrag och att sanktionsavgifter därför kan leda till att ytterligare medel måste tillföras, vilket skapar en rundgång i statskassan. Vidare framför bl.a. *Polismyndigheten* och *Försäkringskassan* att det i den offentliga sektorn − i motsats till den privata sektorn – redan finns en straffrättslig sanktion i form av tjänstefelsansvar, vilket vid sidan av möjligheten att vidta disciplinära åtgärder utgör ett skydd mot att enskilda tjänstemän i offentlig verksamhet gör sig skyldiga till grövre överträdelser. Dessutom påpekar de att myndigheten kan bli skadeståndsskyldig gentemot de registrerade.

Dessa invändningar skulle kunna framföras mot alla former av sanktionsavgifter mot myndigheter. Som framgår av utredningens redogörelse har det dock på flera andra områden ansetts utgöra en effektiv och nödvändig sanktion att kunna rikta viten och sanktionsavgifter mot statliga och kommunala myndigheter. Som exempel kan nämnas vite enligt diskrimineringslagen och upphandlingsskadeavgift enligt lagen (2016:1145) om offentlig upphandling. I detta sammanhang förtjänar det också att nämnas att EU-kommissionen har föreslagit att sanktionsavgifter ska kunna tas ut av EU-institutionerna och andra unionsorgan vid överträdelser av den förordning som reglerar bl.a. institutionernas egen behandling av personuppgifter, parallellt med disciplinära påföljder för den ansvarige tjänstemannen (COM(2017) 8 final).

Vidare måste den enskildes intresse av skydd för sin personliga integritet anses väga lika tungt då uppgifter behandlas i det allmännas verksamhet som då behandlingen sker i den privata sektorn. För att utföra sina uppgifter måste såväl statliga som kommunala myndigheter behandla mycket stora mängder personuppgifter, ofta av känslig karaktär. Denna behandling måste givetvis ske i enlighet med dataskyddsregleringen. Vid tillsynsmyndigheternas granskning under senare år har det dock framkommit fall där myndigheter begått förhållandevis allvarliga överträdelser av dataskyddsregleringen. Det kan alltså inte tas för givet att myndigheter alltid följer regleringen om dataskydd.

Tjänstefelsansvar eller disciplinansvar på individnivå är enligt regeringens mening inte tillräckligt effektiva sanktioner mot systematiska överträdelser. För att komma till rätta med sådana överträdelser krävs ofta investeringar i förbättrad teknik eller tydliga riktlinjer från myndighetens högsta ledning. Vetskapen om att brister i personuppgiftsbehandlingen skulle kunna leda till att höga sanktionsavgifter påförs, kommer enligt regeringens bedömning att leda till att myndighetsledningen, i normalfallet, tillser att åtgärder vidtas för att regleringen ska följas. Beslut om att faktiskt påföra en myndighet sanktionsavgifter torde därmed mycket sällan behöva komma i fråga. Sanktionsavgifter skulle således fylla en viktig preventiv funktion, även när det gäller myndigheter, och innebära en verklig förstärkning av integritetsskyddet för enskilda. Denna effekt kan inte enbart uppnås genom skadeståndsinstitutet, eftersom detta är beroende av att den registrerade driver en skadeståndstalan.

Sammanfattningsvis menar regeringen, liksom utredningen, att övervägande skäl talar för att sanktionsavgifter ska kunna tas ut av statliga och kommunala myndigheter vid överträdelser av bestämmelserna i dataskyddsförordningen.

Bestämmelsen i artikel 83.7 om medlemsstaternas möjligheter att bestämma i vilken utsträckning myndigheter ska kunna påföras avgifter innebär att medlemsstaterna har utrymme att bestämma ett tak för de belopp som kan påföras myndigheter. Visserligen kan det, i enlighet med vad *Företagarna* och *Stiftelsen för internetinfrastruktur* anför, framstå som rimligt att samma typ av överträdelse leder till samma typ av sanktion, oavsett om överträdelsen begåtts av en myndighet eller ett privat subjekt. Regeringen anser dock, i likhet med utredningen, att det maximala belopp som ska kunna påföras myndigheter bör ligga i paritet med andra sanktionsavgifter i svensk rätt och därmed vara väsentligt lägre än det högsta belopp som skulle kunna tas ut av ett företag enligt dataskyddsförordningen. Inom den privata sektorn kan en överträdelse av dataskyddsregleringen, förutom att kränka enskildas personliga integritet, medföra otillbörliga konkurrensfördelar som snedvrider den inre marknaden. Någon sådan ekonomisk vinning, på bekostnad av andra aktörer på marknaden, kan myndigheter inte dra. Här kan också noteras att i kommissionens förslag till den förordning som reglerar institutionernas och unionsorganens egen behandling av personuppgifter sätts beloppsgränsen för sanktionsavgifterna betydligt lägre än enligt dataskyddsförordningen. En institution ska enligt förslaget kunna påföras sanktionsavgifter om maximalt 500 000 euro per år.

Sanktionsavgifter ska enligt dataskyddsförordningen tas ut enligt två olika nivåer – en lägre nivå vid överträdelser som betraktas som mindre allvarliga och en högre nivå vid allvarligare överträdelser och underlåtenhet att följa förelägganden eller beslut av tillsynsmyndigheten eller att på annat sätt bistå den. Även för myndigheter finns det skäl att ha två olika avgiftsnivåer. Utredningen föreslår att ett maxbelopp om 10 000 000 kronor ska kunna påföras för mindre allvarliga överträdelser. För allvarliga överträdelser föreslår utredningen att maxbeloppet ska vara 20 000 000 kronor. Vissa remissinstanser, t.ex. *Centrala studiestödsnämnden*, anser att beloppen är orimliga och främmande för svensk förvaltningstradition. *Trafikverket* påpekar att 20 000 000 kronor är dubbelt så mycket som den högsta sanktionsavgift som kan påföras en svensk myndighet enligt gällande rätt.

Det kan konstateras att 10 000 000 kronor är vad som i dag maximalt kan påföras en myndighet i upphandlingsskadeavgift. Regeringen anser att högre belopp än så inte heller bör kunna påföras en myndighet vid överträdelser av dataskyddsförordningen. Enligt regeringens bedömning skulle en avgift om 10 000 000 kronor utgöra en effektiv, proportionell och avskräckande sanktion också mot allvarliga överträdelser av förordningen, även för de allra största myndigheterna.

Det finns, utifrån förordningens modell, skäl att bestämma beloppen för mindre allvarliga överträdelser till hälften, dvs. 5 000 000 kronor. Vid bestämmandet av vad som utgör en mindre allvarlig respektive en allvarlig överträdelse bör förordningens artikel 83.4 respektive 83.5 gälla.

I förordningens artikel 83.1–3 anges vilka omständigheter som ska beaktas vid beslut om att ta ut sanktionsavgifter och vid bestämmande av beloppets storlek. Dessa bestämmelser bör tillämpas även då sanktionsavgifter tas ut av myndigheter. Detta innebär att en avgift kan påföras med allt ifrån 0 kronor upp till maxbeloppet, beroende på vad som i det enskilda fallet är lämpligt med hänsyn till de olika omständigheter som anges i artikel 83.1–2.

Skolverket, *Sveriges Kommuner och Landsting* och flera kommuner påpekar i detta sammanhang att en hög sanktionsavgift kan komma att slå orimligt hårt mot mindre myndigheter. Enligt artikel 83.2 a ska dock vederbörlig hänsyn tas till bl.a. den aktuella personuppgiftsbehandlingens omfattning och antalet berörda registrerade. Eftersom små myndigheter ofta behandlar färre personuppgifter innebär detta i praktiken att myndighetens storlek kan få betydelse när avgiften bestäms. Vidare ska tillsynsmyndigheten, enligt artikel 83.1, säkerställa att påförande av administrativa sanktionsavgifter i varje enskilt fall är effektivt, proportionellt och avskräckande. Även denna bestämmelse innebär att tillsynsmyndigheten måste, i enlighet med den proportionalitetsprincip som gäller vid all myndighetsutövning, anpassa avgiftens storlek till den aktuella myndighetens budgetram.

Sammanfattningsvis föreslår regeringen att tillsynsmyndigheten ska få ta ut sanktionsavgifter även av statliga och kommunala myndigheter vid överträdelser av bestämmelserna i dataskyddsförordningen. För mindre allvarliga överträdelser bör avgiften uppgå till högst 5 000 000 kronor och för allvarligare överträdelser till högst 10 000 000 kronor. Vid bestämmandet av avgiftens storlek i det enskilda fallet bör dataskyddsförordningens bestämmelser tillämpas. Med hänsyn till behovet av

förutsebarhet i fråga om vilka sanktioner som kan bli följden av överträdelser, bör hänvisningen till dataskyddsförordningen i denna bestämmelse vara statisk, dvs. avse förordningen i den ursprungliga lydelsen.

16.3 Övriga sanktioner

16.3.1 Medlemsstaternas skyldigheter

Enligt artikel 84 i förordningen ska medlemsstaterna fastställa regler om andra sanktioner för överträdelser av förordningen, särskilt för sådana som inte är föremål för administrativa sanktionsavgifter. Sanktionerna ska enligt artikeln vara effektiva, proportionella och avskräckande. I skäl 152 anges att medlemsstaterna bör genomföra ett system med effektiva, proportionella och avskräckande sanktioner om förordningen inte harmoniserar administrativa sanktioner eller om det är nödvändigt i andra fall. Det anges också i nämnda skäl att det ska fastställas om sanktionerna ska vara av straffrättslig eller administrativ art.

I skäl 149 anges att medlemsstaterna bör kunna fastställa bestämmelser om straffrättsliga påföljder och möjligheter att förverka den vinning som gjorts vid överträdelser av förordningen. Där erinras också om att utdömandet av sådana påföljder och administrativa sanktioner inte bör medföra ett åsidosättande av dubbelprövningsförbudet enligt EU-domstolens tolkning.

De sanktionsverktyg som normalt står till buds för staten är främst straff och sanktionsavgifter samt vite och återkallelse av tillstånd. Förordningen föreskriver dock inte något sådant tillståndsförfarande som gör att återkallelse kan användas som sanktion.

16.3.2 Straff och vite

Regeringens bedömning: Överträdelser av EU:s dataskyddsförordning bör inte vara straffsanktionerade.

Någon möjlighet för tillsynsmyndigheten att förena sina förelägganden med vite bör inte införas.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Alla remissinstanser utom *Migrationsverket* och *Dataskydd.net* instämmer i utredningens bedömning eller kommenterar den inte. Migrationsverket anser att det åtminstone bör övervägas om inte sanktionsavgifterna behöver kompletteras med straffbestämmelser för att motverka otillåten och riskfylld personuppgiftsbehandling. Dataskydd.net delar inte utredningens bedömning att viten inte bör ställas till tillsynsmyndighetens förfogande.

Skälen för regeringens bedömning

Straff

Enligt 49 § PUL är vissa bestämmelser i lagen förenade med straffansvar. Utredningen konstaterar att straffbestämmelsen har tillämpats sparsamt under senare tid.

Vid sidan av straffbestämmelsen i personuppgiftslagen finns andra straffbestämmelser som också kan innebära att vissa gärningar som innefattar personuppgiftsbehandling omfattas av straffansvar – såsom bestämmelserna om dataintrång (4 kap. 9 c § brottsbalken), kränkande fotografering (4 kap. 6 a § brottsbalken), förtal (5 kap. 1 § brottsbalken) och tjänstefel (20 kap. 1 § brottsbalken).

I prop. 2016/17:222 föreslår regeringen att ett nytt gradindelat brott införs i brottsbalken, olaga integritetsintrång. Regleringen straffbelägger intrång i någons annans privatliv genom spridning av vissa slag av bilder eller andra uppgifter, om spridningen är ägnad att medföra allvarlig skada för den som bilden eller uppgiften rör. Om gärningen med hänsyn till bildens eller uppgiftens innehåll eller sättet för eller omfattningen av spridningen var ägnad att medföra mycket allvarlig skada för den som bilden eller uppgiften rör, döms för grovt olaga integritetsintrång. Straffet för olaga integritetsintrång föreslås vara böter eller fängelse i högst två år och för grovt olaga integritetsintrång fängelse i lägst sex månader och högst fyra år. Undantag från straffansvar ska gälla om gärningen med hänsyn till syftet och övriga omständigheter var försvarlig.

Kriminalisering som metod för att försöka hindra överträdelser av olika normer i samhället bör användas med försiktighet. Ett skäl till detta är att en alltför omfattande kriminalisering riskerar att undergräva straffsystemets brottsavhållande verkan, särskilt om rättsväsendet inte kan beivra alla brott på ett effektivt sätt. Ett annat skäl är att kriminalisering innebär påtagliga inskränkningar i medborgarnas valfrihet och ingripande tvångsåtgärder mot dem som begår brott.

När det gäller överträdelser av dataskyddsregleringen utgör straff inte en särskilt effektiv sanktion, eftersom det i många fall är svårt att identifiera en fysisk person som ansvarig för överträdelsen samt att leda i bevis att denne haft uppsåt eller varit oaktsam på det sätt som krävs för straffbarhet. Den omständigheten att den personuppgiftsansvarige eller personuppgiftsbiträdet kan påföras höga sanktionsavgifter vid brott mot regelverket bör ha en väsentligt högre avskräckande effekt och leda till att efterlevnaden av regelverket prioriteras högt. Vidare kan införandet av straff aktualisera det dubbelprövningsförbud som gäller enligt Europakonventionen och EU:s stadga om de grundläggande rättigheterna samt göra det svårt för personuppgiftsansvariga att förutse vilken sanktion som kan komma ifråga för vilken överträdelse. Vid sidan av systemet med sanktionsavgifter finns också det i det närmaste strikta skadeståndsansvar som gäller enligt förordningens artikel 82, vilket också får antas ha en avskräckande effekt.

Dessa omständigheter talar enligt regeringens bedömning för att överträdelser av dataskyddsförordningen inte behöver straffsanktioneras och att det till och med skulle kunna vara olämpligt. *Migrationsverket* anser dock att det åtminstone bör övervägas om inte sanktionsavgifterna behöver kompletteras med straffbestämmelser för att motverka otillåten

och riskfylld personuppgiftsbehandling. Regeringen vill i detta sammanhang betona att vissa beteenden som innefattar personuppgiftsbehandling redan är straffsanktionerade enligt andra bestämmelser, såsom exempelvis tjänstefel, dataintrång och förtal. Dessutom kommer det nya brottet olaga integritetsintrång att kunna aktualiseras i vissa fall. Integritetskränkningar som begås vid personuppgiftsbehandling kommer således inte att sakna straffrättsliga sanktioner.

Sammanfattningsvis anser regeringen att det system med sanktionsavgifter som införs genom dataskyddsförordningen utgör en tillräckligt effektiv och avskräckande sanktion mot överträdelser av regelverket. Regeringen föreslår därför ingen straffbestämmelse.

Vite

Enligt 44 och 45 §§ PUL får Datainspektionen vid vite förbjuda en personuppgiftsansvarig att fortsätta att behandla uppgifter på annat sätt än att lagra dem, om inspektionen inte på begäran får tillgång till ett tillräckligt underlag för att konstatera att behandlingen är laglig eller om tillsynsmyndigheten konstaterar att personuppgifter behandlas eller kan komma att behandlas på ett olagligt sätt. Detsamma gäller om den personuppgiftsansvarige inte frivilligt följer ett beslut om säkerhetsåtgärder. Bestämmelserna om vite gäller även för statliga och kommunala myndigheter som är personuppgiftsansvariga. Utredningen konstaterar att Datainspektionen aldrig har utnyttjat möjligheten att vitesföreläggа.

Som nämns ovan kan sanktionsavgifterna enligt förordningen användas framåtsyftande, dvs. för att säkerställa ett agerande i enlighet med tillsynsmyndighetens pålagor, genom att det erinras om att sanktionsavgifter kan utgå enligt artikel 83.5 e och artikel 83.6 om föreläggandet eller beslutet inte följs. Regeringen bedömer, till skillnad från *dataskydd.net*, att denna möjlighet bör fylla tillsynsmyndighetens behov av handlingsdirigerande sanktion, och att det därför inte finns något behov för tillsynsmyndigheten att också kunna förena sina förelägganden med vite på förordningens tillämpningsområde. Det faktum att dubbelprövningsförbudet kan aktualiseras även då vite utdöms för gärningar som också kan leda till sanktionsavgifter, talar ytterligare emot att införa en sådan möjlighet. Regeringen instämmer därför i utredningens bedömning att en möjlighet för tillsynsmyndigheten att förena sina förelägganden med vite inte bör införas.

16.3.3 Sanktionsavgift och uppgifter om lagöverträdelser

Regeringens förslag: Tillsynsmyndigheten får ta ut sanktionsavgifter enligt EU:s dataskyddsförordning även vid överträdelser av förordningens bestämmelser om behandling av personuppgifter som rör lagöverträdelser. Avgiftens storlek ska bestämmas inom ramen för den högre beloppsgräns som gäller för överträdelser av bl.a. bestämmelserna om känsliga personuppgifter.

Utredningens förslag överensstämmer i huvudsak med regeringens. Utredningen föreslår att bestämmelsens hänvisning till dataskydds-

förordningen ska vara dynamisk, se avsnitt 5.1.2. Utredningens förslag har även en delvis annan utformning.

Remissinstanserna: Det stora flertalet remissinstanser tillstyrker förslaget eller har inga synpunkter på det. Några remissinstanser, bl.a. *Svenskt Näringsliv*, *Svensk Handel*, *Svensk Försäkring*, *Teknikföretagen*, *Säkerhets- och försvarsföretagen* och *Näringslivets regelnämnd*, avstyrker förslaget. *Svensk Försäkring* avstyrker förslaget eftersom bestämmelserna om behandling av uppgifter som rör lagöverträdelser föreslås omfatta även misstanke om brott. Teknikföretagen och Säkerhets- och försvarsföretagen påpekar att förslaget enbart kommer att drabba privata aktörer och menar att detta skulle kunna innebära en kraftig konkurrensbegränsning i förhållande till andra EU-länder. Vissa remissinstanser, bl.a. Svenskt Näringsliv, anser att förslaget utgör en överimplementering av förordningen samt betonar näringslivets intresse av harmonisering för att kunna konkurrera på lika villkor. Näringslivets regelnämnd anser att förslaget utgör en överimplementering som kan få negativa konsekvenser för företagen och som därför måste motiveras och konsekvensutredas.

Skälen för regeringens förslag: Enligt personuppgiftslagen är regleringen om behandling av personuppgifter som rör lagöverträdelser straffsanktionerad på samma sätt som regleringen om känsliga personuppgifter (46 § PUL). Dataskyddsförordningens bestämmelser om sanktionsavgifter gäller däremot inte vid överträdelser av den bestämmelse i förordningen som avser behandling av personuppgifter som rör lagöverträdelser, dvs. artikel 10. Om inga sanktioner införs på nationell nivå mot sådana överträdelser skulle alltså integritetsskyddet försämras jämfört med vad som gäller enligt personuppgiftslagen. Dessutom är medlemsstaterna enligt artikel 84.1 skyldiga att fastställa regler om effektiva, proportionella och avskräckande sanktioner för överträdelser som inte är föremål för administrativa sanktionsavgifter enligt artikel 83. En sådan sanktion måste således införas mot överträdelser av artikel 10. Utredningens förslag utgör därmed inte, som bl.a. *Svenskt Näringsliv* anför, en överimplementering av förordningen.

Som framgår av föregående avsnitt anser regeringen att överträdelser av förordningen inte bör vara straffsanktionerade. Detta gäller även vid överträdelser mot artikel 10. Frågan är således vilken annan sanktion som bör införas vid behandling av personuppgifter om lagöverträdelser i strid med förordningen.

Regeringen anser att intresset av att upprätthålla efterlevnaden av de begränsningar som anges i artikel 10 väger lika tungt ur integritetssynpunkt som att säkerställa efterlevnaden av förbudet mot behandling av vissa typer av känsliga personuppgifter. Behandling av uppgifter som rör t.ex. fällande domar i brottmål uppfattas många gånger som lika integritetskänslig av den registrerade. Detta talar för att samma system för sanktionsavgifter bör gälla vid överträdelser av artikel 10 som vid överträdelser av regleringen om känsliga personuppgifter i artikel 9.

Flera remissinstanser som företräder näringslivet, bl.a. *Teknikföretagen* och Svenskt Näringsliv, poängterar vikten av harmonisering och menar att det skulle utgöra en konkurrensnackdel för svenska företag om sanktionsavgifter infördes i svensk rätt vid överträdelser av artikel 10. Regeringen kan dock konstatera att samtliga medlemsstater, till följd av

kravet i artikel 84.1, kommer att behöva införa någon form av effektiv, proportionell och avskräckande sanktion mot överträdelser av artikel 10. Ett genomförande av utredningens förslag bör därmed inte kunna leda till den snedvridning av marknaden som dessa remissinstanser befarar.

Regeringen föreslår således att tillsynsmyndigheten ska få ta ut sanktionsavgifter enligt dataskyddsförordningen även vid överträdelser av artikel 10 i dataskyddsförordningen. Avgiftens storlek ska i enlighet med utredningens förslag bestämmas inom ramen för den högre beloppsgräns som gäller för överträdelser av bl.a. bestämmelserna om känsliga personuppgifter, dvs. med tillämpning av artikel 83.5 i förordningen. Med hänsyn till behovet av förutsebarhet i fråga om vilka sanktioner som kan bli följden av överträdelser, bör hänvisningen till dataskyddsförordningen i denna bestämmelse vara statisk, dvs. avse förordningen i den ursprungliga lydelsen.

16.4 Förfarandebestämmelser om sanktionsavgift

Regeringens förslag: En sanktionsavgift får inte tas ut om den som anspråket riktas mot inte har getts tillfälle att yttra sig inom fem år från det att överträdelsen ägde rum. Ett beslut om sanktionsavgift ska delges.

Sanktionsavgifter ska tillfalla staten. En sanktionsavgift ska betalas till tillsynsmyndigheten inom 30 dagar från det att beslutet om att ta ut avgiften har fått laga kraft eller inom den längre tid som anges i beslutet. Om sanktionsavgiften inte betalas inom denna tid, ska tillsynsmyndigheten lämna den obetalda avgiften för indrivning. Vid indrivning får verkställighet ske enligt utsökningsbalken.

Regeringen får meddela ytterligare föreskrifter om sanktionsavgifter enligt EU:s dataskyddsförordning och dataskyddslagen.

Utredningens förslag överensstämmer i sak med regeringens. Utredningen föreslår inte något bemyndigande för regeringen att meddela ytterligare föreskrifter. Vidare föreslår utredningen att bestämmelsen om betalning och indrivning av sanktionsavgift ska införas i förordning och inte i dataskyddslagen.

Remissinstanserna: Det stora flertalet remissinstanser tillstyrker förslaget eller har inga synpunkter på det. Bland andra *Svensk Handel* och *Svenskt Näringsliv* anser dock att preskriptionstidens längd bör begränsas till tre år.

Skälen för regeringens förslag: Beslut om administrativa sanktionsavgifter är en särskilt ingripande åtgärd. Sådana beslut bör därför delges den betalningsskyldige enligt delgivningslagen (2010:1932). Av samma skäl bör beslut om sanktionsavgifter inte få fattas om lång tid har förflutit sedan överträdelsen ägde rum. Någon preskriptionstid anges dock inte i dataskyddsförordningen. En sådan begränsning av tillsynsmyndighetens befogenheter måste i stället anses ingå i medlemsstaternas skyldighet att ställa upp lämpliga skyddsåtgärder för rättssäkerheten i nationell rätt (artikel 58.4).

Utredningen föreslår att en sanktionsavgift inte ska få tas ut om den som anspråket riktas mot inte inom fem år från det att överträdelsen ägde

rum har getts tillfälle att yttra sig. Några remissinstanser, bl.a. *Svensk Handel* och *Svenskt Näringsliv*, anser att denna preskriptionstid är för lång och att den i stället bör vara tre år. Regeringen anser emellertid, i likhet med utredningen, att preskriptionstidens längd bör bestämmas i enlighet med vad som gäller för t.ex. miljösanktionsavgift, dvs. till fem år.

Det framgår inte av dataskyddsförordningen om de sanktionsavgifter som kan komma att tas ut ska betalas till EU eller till medlemsstaterna. Inte heller regleras det i förordningen hur betalningen eller den närmare verkställigheten av avgifterna ska ske. I avsaknad av reglering i förordningen om vem sanktionsavgifterna tillfaller, måste utgångspunkten vara att avgifterna ska tillfalla staten. Detta bör framgå av dataskyddslagen.

Utredningen anser att det bör lämnas till regeringen att bestämma till vilken myndighet betalning ska ske. Regeringen gör ingen annan bedömning. Vidare föreslår utredningen att den till dataskyddslagen anslutande förordningen ska innehålla vissa bestämmelser om betalning och indrivning av sanktionsavgifter. Bland annat anges i utredningens förslag till förordning att sanktionsavgift ska betalas inom 30 dagar från det att beslutet om att ta ut avgiften har fått laga kraft eller inom den längre tid som anges i beslutet. Om sanktionsavgiften inte betalas inom denna tid, föreslås att myndigheten ska lämna den obetalda avgiften för indrivning samt att verkställighet får ske enligt utsökningsbalken. Den bestämmelsen bör enligt regeringens mening tas in i dataskyddslagen.

Utredningen bedömer att föreskrifter om verkställighet av sanktionsavgifter kan meddelas av regeringen eller den myndighet regeringen bestämmer med stöd av 8 kap. 7 § RF. Regeringen anser dock att det sannolikt kommer att behövas föreskrifter om sanktionsavgifter som går utöver vad som omfattas av denna normgivningskompetens. Det behövs därför ett bemyndigande i dataskyddslagen som anger att regeringen får meddela ytterligare föreskrifter om sanktionsavgifter enligt dataskyddsförordningen och dataskyddslagen.

17 Rättsmedel och processuella frågor

17.1 Rättsmedel mot den personuppgiftsansvarige eller personuppgiftsbiträdet

17.1.1 Rätt att föra talan om ersättning

Regeringens förslag: Rätten till ersättning från den personuppgiftsansvarige och personuppgiftsbiträdet enligt EU:s dataskyddsförordning gäller vid överträdelser av bestämmelser i dataskyddslagen och andra föreskrifter som kompletterar dataskyddsförordningen.

Utredningens förslag överensstämmer i sak med regeringens.

Remissinstanserna: Det stora flertalet remissinstanser tillstyrker utredningens förslag eller har inga synpunkter på det. *Vetenskapsrådet*

välkomnar utredningens förslag att införa en bestämmelse om skadestånd som omfattar övriga tillämpliga författningar. *Justitiekanslern* anser att den föreslagna lagtexten rörande skadestånd möjligen utvidgar skadeståndsansvaret i förhållande till vad som krävs enligt dataskyddsförordningen. *Lunds universitet* ifrågasätter om formuleringen andra författningar som kompletterar dataskyddsförordningen är tillräckligt precis. *Svensk Handel* anser att det finns ett behov av en preskriptionstid för skadeståndsanspråk.

Skälen för regeringens förslag

Rätten till ersättning gäller vid överträdelser av dataskyddslagen och sektorsspecifika föreskrifter

Enligt 48 § PUL ska den personuppgiftsansvarige ersätta den registrerade för skada och kränkning av den personliga integriteten som en behandling av personuppgifter i strid med personuppgiftslagen har orsakat. Bestämmelsen gäller endast vid behandling i strid med personuppgiftslagen och alltså inte vid behandling i strid med sektorsspecifik lagstiftning. Många sektorsspecifika författningar innehåller emellertid en hänvisning till skadeståndsbestämmelsen i personuppgiftslagen.

I dataskyddsförordningen regleras rätten till ersättning genom en direkt tillämplig bestämmelse, som tar över de allmänna skadeståndsreglerna i skadeståndslagen (1 kap. 1 §). Enligt artikel 82 ska varje person som har lidit materiell eller immateriell skada till följd av en överträdelse av förordningen ha rätt till ersättning från den personuppgiftsansvarige eller personuppgiftsbiträdet för den uppkomna skadan. Enligt dataskyddsförordningen kan således även personuppgiftsbiträden bli skadeståndsskyldiga under vissa förutsättningar. Ersättningen ska täcka såväl materiell som immateriell skada, dvs. med svenska termer ekonomisk och ideell skada. Kränkning, som i 48 § PUL nämns särskilt vid sidan av skada, får anses utgöra en immateriell skada. I skäl 146 och artikel 82.2–5 preciseras närmare under vilka förutsättningar personuppgiftsansvariga och personuppgiftsbiträden kan hållas ansvariga för uppkomna skador. Domstolsförfaranden rörande skadestånd ska enligt artikel 82.6 tas upp vid de domstolar som är behöriga enligt artikel 79.2, dvs. vid en domstol i den medlemsstat där den personuppgiftsansvarige eller personuppgiftsbiträdet är etablerad. Såvida den ansvarige eller biträdet inte är en myndighet får talan i stället väckas vid en domstol i den medlemsstat där den registrerade har sin hemvist. Bestämmelsen tar över rättegångsbalkens allmänna forumregler (10 kap. 21 § rättegångsbalken).

Dataskyddsförordningen innehåller inte någon reglering om preskriptionstid för skadeståndsanspråk som riktas mot den personuppgiftsansvarige eller personuppgiftsbiträdet. Någon särskild föreskriven preskriptionsfrist finns inte heller för skadeståndsanspråk enligt personuppgiftslagen. Det är i stället de allmänna reglerna i preskriptionslagen (1981:130) som gäller. Regeringen anser till skillnad från *Svensk Handel* inte att det framkommit skäl att införa särskilda regler om preskription för ersättning enligt dataskyddsförordningen.

Enligt ordalydelsen i artikel 82 gäller rätten till ersättning vid skada som uppstått till följd av behandling som strider mot dataskyddsförordningen. Med detta uttryck avses dock enligt skäl 146 även behand-

ling som strider mot nationella bestämmelser som närmare specificerar förordningens bestämmelser. Regeringen anser, i likhet med utredningen, att detta bör förtydligas i dataskyddslagen genom en bestämmelse som upplyser om att rätten till ersättning gäller även vid överträdelser av bestämmelser i dataskyddslagen och andra föreskrifter som kompletterar dataskyddsförordningen. Till skillnad från *Lunds universitet* anser regeringen att den av utredningen föreslagna avgränsningen är tillräckligt tydlig, eftersom dataskyddsförordningen reglerar gränserna för vad som får regleras i nationell rätt. Sådana föreskrifter som kompletterar förordningen och som skulle kunna läggas till grund för ersättningsanspråk enligt artikel 82 är enligt regeringens bedömning av det slaget att de fastställer mer specifika krav för behandlingen av personuppgifter, på det sätt som anges i t.ex. artikel 6.2 och 6.3 andra stycket i dataskyddsförordningen.

Bestämmelsen innebär emellertid, som *Justitiekanslern* påpekar, en viss utvidgning av rätten till ersättning jämfört med vad som gäller enligt dataskyddsförordningen. Eftersom dataskyddsförordningens tillämpningsområde utsträcks genom dataskyddslagen till att gälla även i verksamhet som inte omfattas av unionsrätten, kommer rätten till ersättning också som huvudregel att gälla vid överträdelser av sektorsspecifika bestämmelser som kompletterar förordningen inom det utsträckta området. Bestämmelsen utgör även en viss utvidgning av rätten till ersättning jämfört med vad som gäller i dag, eftersom den omfattar överträdelser av bestämmelser i alla sektorsspecifika författningar och inte bara de som särskilt reglerar denna fråga. Detta, vilket är en följd av bestämmelsen i artikel 82 så som den ska tolkas enligt skäl 146, utgör enligt regeringens mening en förstärkning av integritetsskyddet och av den registrerades tillgång till effektiva rättsmedel.

17.1.2 Rätt att överklaga en myndighets beslut om personuppgiftsbehandling

Regeringens förslag: Om den personuppgiftsansvarige är en myndighet, får beslut som myndigheten fattar enligt EU:s dataskyddsförordning med anledning av att en registrerad utövar sin rätt till information och tillgång till personuppgifter, rättelse, radering, begränsning, invändning eller dataportabilitet överklagas till allmän förvaltningsdomstol. Detta gäller inte beslut av regeringen, Högsta domstolen, Högsta förvaltningsdomstolen eller Riksdagens ombudsmän.

Andra beslut som en personuppgiftsansvarig myndighet fattar enligt dataskyddsförordningen får inte överklagas.

Utredningens förslag överensstämmer delvis med regeringens. Utredningen föreslår inte att beslut om dataportabilitet ska anges i bestämmelsen om överklagande av myndighetsbeslut. Vidare anges även riksdagen i utredningens förslag till undantag. Slutligen föreslår utredningen inte något uttryckligt överklagandeförbud i fråga om andra beslut som meddelas enligt dataskyddsförordningen.

Remissinstanserna: Det stora flertalet remissinstanser tillstyrker utredningens förslag eller har inga synpunkter på det. *Pensionsmyndigheten* och *Sveriges advokatsamfund* anser att det bör framgå att även beslut om dataportabilitet får överklagas. *Dataskydd.net* anser att även beslut enligt artiklarna 14.5 b–d och 22 ska kunna överklagas. *Förvaltningsrätten i Stockholm* saknar överväganden kring, eller en förklaring till, varför de båda högsta domstolsinstansernas beslut har undantagits från rätten att överklaga beslut.

Skälen för regeringens förslag: Om den personuppgiftsansvarige är en myndighet får enligt gällande rätt vissa av de beslut som myndigheten fattar i denna egenskap överklagas till allmän förvaltningsdomstol (52 § PUL). Denna rätt gäller endast myndighetens beslut om information enligt 26 § PUL, om rättelse och underrättelse till tredje man enligt 28 §, om information enligt 29 § andra stycket och om upplysningar enligt 42 §. Bestämmelsen har inte sin grund i dataskyddsdirektivet, utan motiveras av allmänna förvaltningsrättsliga principer om att förvaltningsbeslut som direkt berör en enskild person ska kunna överprövas av domstol (prop. 2005/06:173 s. 51–53).

När den personuppgiftsansvarige är en myndighet kan vissa beslut som meddelas till följd av en begäran av en registrerad sägas vara ett utflöde av myndighetens myndighetsutövning. Sådana beslut bör därför kunna överklagas av den registrerade. I den mån myndigheten omfattas av förvaltningslagens tillämpningsområde är besluten överklagbara enligt allmänna förvaltningsrättsliga principer. När den nya förvaltningslagen träder i kraft kommer rätten att överklaga sådana beslut att följa direkt av den lagen. Det behövs därmed i och för sig inte någon uttrycklig bestämmelse om rätten att överklaga beslut som fattas enligt dataskyddsförordningen i dataskyddslagen. Beslut enligt dataskyddsförordningen kommer emellertid att fattas av personuppgiftsansvariga myndigheter även i andra fall än till följd av att en registrerad utövar sina rättigheter. Sådana andra beslut, t.ex. om att utnämna ett dataskyddsombud eller att anmäla en personuppgiftsincident, bör inte vara överklagbara.

Dataskyddslagen bör därför, i likhet med personuppgiftslagen, förses med en uttrycklig bestämmelse om att endast vissa myndighetsbeslut får överklagas till allmän förvaltningsdomstol. Prövningstillstånd bör krävas vid överklagande till kammarrätten.

Enligt 52 § PUL gäller rätten att överklaga inte sådana beslut som har fattats av riksdagen, regeringen eller riksdagens ombudsmän. Utredningen föreslår att denna begränsning bör gälla även enligt dataskyddslagen. Eftersom riksdagen inte utgör en myndighet enligt svensk rätt behöver den dock inte undantas. Utredningen föreslår därutöver att beslut som fattas av de högsta domstolsinstanserna ska undantas. Som *Förvaltningsrätten i Stockholm* påpekar lämnas ingen motivering till detta i betänkandet. Regeringen kan dock konstatera att Högsta domstolen är högsta allmänna domstol och Högsta förvaltningsdomstolen är högsta förvaltningsdomstol (11 kap. 1 § RF). Av detta följer att dessa domstolars avgöranden inte kan överklagas. Högsta domstolens och Högsta förvaltningsdomstolens egna beslut enligt dataskyddsförordningen bör därför inte kunna överklagas. Detta överensstämmer med vad som gäller enligt bl.a. offentlighets- och sekretesslagen (6 kap. 7 § tredje stycket OSL). Regeringen anser därför att beslut från regeringen, Riksdagens

ombudsmän och de högsta domstolarna ska undantas från rätten att överklaga.

Rätten att överklaga bör omfatta beslut som en personuppgiftsansvarig myndighet fattar med anledning av att en registrerad utövar sina rättigheter enligt kapitel III i dataskyddsförordningen. De bestämmelser som kan föranleda överklagbara beslut rör enligt utredningens bedömning avgifter m.m. (artikel 12.5), tillgång till personuppgifter m.m. (artikel 15), rättelse (artikel 16), radering (artikel 17), begränsning (artikel 18), underrättelse till tredje man om rättelse, radering eller begränsning (artikel 19) och invändningar (artikel 21). Som *Pensionsmyndigheten* och *Sveriges advokatsamfund* påpekar skulle dock i vissa fall även bestämmelsen om dataportabilitet i artikel 20 kunna föranleda beslut av en personuppgiftsansvarig myndighet och bör därför av tydlighetsskäl också anges i den föreslagna bestämmelsen om överklagande. *Dataskydd.net* anser därutöver att bestämmelserna om information i artiklarna 14.5 b–d och om automatiserade beslut i artikel 22 bör omfattas av rätten att överklaga. Regeringen kan dock konstatera att rätten till information inte omfattas av överklagandebestämmelsen i 52 § PUL och att det inte finns skäl att nu införa en annan ordning. När det gäller automatiserade beslut innehåller 52 § PUL visserligen en hänvisning till 29 § andra stycket PUL, som anger att den registrerade har rätt att på begäran få information om vad som har styrt den automatiserade behandling som lett fram till beslutet. Någon sådan rätt till information föreligger emellertid inte enligt artikel 22 i dataskyddsförordningen. Följaktligen bör någon rätt att överklaga beslut enligt artikel 22 inte införas i dataskyddslagen. Vidare bör det av dataskyddslagen framgå att andra beslut som en personuppgiftsansvarig myndighet fattar enligt dataskyddsförordningen inte får överklagas.

17.2 Klagomål till tillsynsmyndigheten

Regeringens bedömning: Det behövs inga särskilda författningsbestämmelser om den registrerades rätt att lämna in klagomål eller om tillsynsmyndighetens skyldigheter att handlägga sådana klagomål inom rimlig tid.

Utredningen föreslår till skillnad från regeringen att särskilda bestämmelser om åtgärder vid dröjsmål ska införas, bl.a. en rätt för den registrerade att föra en dröjsmålstalan i allmän förvaltningsdomstol.

Remissinstanserna: Endast ett fåtal remissinstanser yttrar sig särskilt över utredningens förslag. *Riksdagens ombudsmän*, *Förvaltningsrätten i Jönköping* och *Uppsala universitet* ifrågasätter det praktiska värdet eller behovet av en dröjsmålstalan och anser att frågan bör utredas vidare. *Kammarrätten i Göteborg* anser att den föreslagna ordningen framstår som onödigt komplicerad och överdimensionerad. Även *Justitiekanslern* anser att de föreslagna bestämmelserna framstår som komplicerade, tidsödande och kostnadskrävande i förhållande till vad som rimligen går att uppnå. Det bör därför enligt Justitiekanslerns uppfattning övervägas om inte tillgången till ett effektivt rättsmedel kan säkerställas på något annat sätt. *Lunds universitet* anser att reglerna om dröjsmålstalan bör

samordnas med motsvarande regler i förslaget till ny förvaltningslag. *Swedish Direct Marketing Association* tycker att det är bra att tillsynsmyndigheten ska tvingas lämna besked inom angiven tidsfrist, men anser att det bör övervägas att även den som klagomålet riktats mot ska kunna begära besked på motsvarande sätt som den registrerade.

Skälen för regeringens förslag: Det finns i gällande svensk rätt inga uttryckliga bestämmelser om rätten att framföra klagomål till Datainspektionen. Dataskyddsförordningen ger inte anledning till att införa nationell reglering av rätten att ge in klagomål eftersom den registrerades rätt att lämna in ett sådant klagomål regleras direkt i artikel 77 i förordningen.

Tillsynsmyndighetens skyldighet att behandla sådana klagomål föreskrivs i artikel 57.1 f. Denna skyldighet innefattar att, där så är lämpligt, undersöka den sakfråga som klagomålet gäller. I samma bestämmelse anges också att tillsynsmyndigheten inom rimlig tid ska underrätta den enskilde om hur undersökningen fortskrider och om resultatet. Av artikel 78.2 framgår att den registrerade i normalfallet inte ska behöva vänta mer än tre månader på detta besked. Det finns mot denna bakgrund inte skäl att också i dataskyddslagen ange tillsynsmyndighetens skyldigheter i förhållande till den registrerade.

Enligt artikel 78.2 ska varje registrerad person ha rätt till ett effektivt rättsmedel om tillsynsmyndigheten underlåter att behandla ett klagomål eller att informera den registrerade inom tre månader om hur det fortskrider med klagomålet eller vilket beslut som har fattats med anledning av detta.

Ett uppenbart ogrundat klagomål bör kunna besvaras av tillsynsmyndigheten tämligen omgående, i vart fall inom tre månader. I andra fall kan tillsynsmyndigheten ha anledning att utnyttja sina tillsynsbefogenheter enligt artikel 58.1, t.ex. att beordra den personuppgiftsansvarige att lämna relevant information eller att göra platsbesök. Besked om huruvida sådan tillsyn ska utövas eller inte bör enligt regeringens mening i princip alltid kunna lämnas till den registrerade inom tre månader. I de undantagsfall ett sådant besked inte kan ges bör tillsynsmyndigheten i vart fall kunna lämna besked om hur ärendet fortskrider. Tillsynsmyndighetens informationsplikt gentemot den registrerade är då uppfylld. Artikel 78.2 i dataskyddsförordningen ger inte den registrerade rätt att inom tidsfristen få ett slutligt besked om vilka eventuella åtgärder gentemot den personuppgiftsansvarige som klagomålet i förlängningen leder till. Bestämmelsen i dataskyddsförordningen syftar i stället till att stävja passivitet hos tillsynsmyndigheten och säkerställer att den registrerade hålls underrättad om handläggningen av ärendet.

Vid sidan av dataskyddsförordningens direkt tillämpliga bestämmelser om tillsynsmyndighetens skyldigheter att bl.a. handlägga klagomål gäller skyndsamhetskrav och informationsskyldighet enligt förvaltningslagens allmänna bestämmelser. Såsom utredningen påpekar förekommer det i dag ingen utebliven eller långsam handläggning av klagomål hos den svenska tillsynsmyndigheten. För det undantagsfall att den registrerade ändå inte skulle få något besked från tillsynsmyndigheten rörande klagomålet inom rimlig tid, kan den registrerade vända sig till Riksdagens ombudsmän och göra en anmälan om brister i handläggningen. Riksdagens ombudsmän har också befogenhet att väcka åtal om tjänste-

fel. Om den registrerade anser att tillsynsmyndighetens dröjsmål lett till skada kan denne också begära skadestånd enligt skadeståndslagen, antingen genom att väcka talan i allmän domstol eller genom att framställa kravet direkt till myndigheten. Enligt förordningen (1995:1301) om handläggning av skadeståndsanspråk mot staten kan en skadelidande få ett sådant skadeståndskrav prövat inom ramen för statens frivilliga skadereglering. Slutligen bör det noteras att även 12 § i den nya förvaltningslagen, som ger den enskilde rätt att föra en dröjsmålstalan mot myndigheten vid långsam handläggning, skulle kunna aktualiseras i ett ärende som initierats genom ett klagomål, men då avseende tillsynsmyndighetens slutliga avgörande. Detta förutsätter dock att den registrerade anses ha ställning som part i förvaltningslagens mening (se avsnitt 17.5).

Sammanfattningsvis anser regeringen att det i svensk rätt redan finns effektiva rättsmedel som är tillgängliga för den registrerade om tillsynsmyndigheten inte skulle uppfylla sin informationsskyldighet enligt dataskyddsförordningen. Regeringen anser därför, i likhet med bl.a. *Riksdagens ombudsmän*, *Justitiekanslern* och *Uppsala universitet*, att utredningens förslag om åtgärder vid tillsynsmyndighetens dröjsmål inte bör genomföras.

17.3 En rättssäker handläggning hos tillsynsmyndigheten

17.3.1 Förordningens krav på skyddsåtgärder

I artikel 58.4 anges att utövandet av de befogenheter som tillsynsmyndigheten tilldelas enligt denna artikel ska omfattas av lämpliga skyddsåtgärder, inbegripet effektiva rättsmedel och rättssäkerhet, som fastställs i unionsrätten och i medlemsstaternas nationella rätt i enlighet med stadgan. I artikel 83.8 upprepas kravet på lämpliga skyddsåtgärder avseende tillsynsmyndighetens befogenhet att påföra administrativa sanktionsavgifter. Innebörden av kravet på skyddsåtgärder i tillsynsmyndighetens verksamhet utvecklas i skäl 129 till förordningen.

Förordningens krav på att tillsynsmyndighetens befogenheter ska kringgärdas av skyddsåtgärder innefattar en skyldighet för medlemsstaterna att dels se till att den personuppgiftsansvarige och personuppgiftsbiträdet har tillgång till effektiva rättsmedel, dels skapa förutsättningar för en rättssäker handläggning hos tillsynsmyndigheten. Frågan om effektiva rättsmedel mot tillsynsmyndigheten behandlas i avsnitt 17.5. I detta avsnitt behandlas behovet av åtgärder för att säkerställa en rättssäker handläggning hos tillsynsmyndigheten.

Tillsynsmyndighetens ärendehandläggning och verksamhet i övrigt omfattas givetvis av regeringsformens grundsatser om legalitet och objektivitet. Dessutom gäller förvaltningslagens generella bestämmelser om bl.a. effektivitet, partsinsyn, kommunikations- och motiveringsskyldighet – bestämmelser som alla syftar till att stärka rättssäkerheten. Vid utövandet av de flesta av tillsynsmyndighetens befogenheter står det klart att dessa allmänna och särskilda krav på god förvaltning är till-

räckliga för att säkerställa de krav på myndighetsutövningen som ställs i dataskyddsförordningen. Det bör dock övervägas om vissa av de mer ingripande befogenheterna föranleder att ytterligare skyddsåtgärder införs. Det bör även övervägas om tillsynsmyndighetens befogenheter att ingripa mot överträdelser av nationella bestämmelser som kompletterar dataskyddsförordningen ska regleras.

17.3.2 Tillsynsmyndighetens befogenheter gäller vid tillsyn enligt dataskyddslagen och sektorsspecifika författningar

Regeringens förslag: Tillsynsmyndighetens befogenheter enligt EU:s dataskyddsförordning gäller vid myndighetens tillsyn över att bestämmelserna i dataskyddslagen och andra föreskrifter som kompletterar förordningen följs. Detta innebär inte att tillsynsmyndigheten får ta ut sanktionsavgifter vid andra överträdelser än de som avses i EU:s dataskyddsförordning.

Utredningens förslag överensstämmer i sak med regeringens. Utredningen föreslår inte någon uttrycklig bestämmelse om befogenheten att ta ut sanktionsavgifter.

Remissinstanserna tillstyrker utredningens förslag eller har inga synpunkter på det. *Förvaltningsrätten i Stockholm* föreslår att Datainspektionen ges uppgiften att vara tillsynsmyndighet genom en bestämmelse i lagen.

Skälen för regeringens förslag: Dataskyddsförordningen innehåller direkt tillämpliga bestämmelser om tillsynsmyndighetens befogenheter. Dessa befogenheter är fler, eller i vart fall mer detaljerat reglerade, än de som anges i personuppgiftslagen. Tillsynsmyndighetens utredningsbefogenheter, som regleras i artikel 58.1 i förordningen, motsvarar i stora drag de befogenheter som myndigheten har enligt personuppgiftslagen. De s.k. korrigerande befogenheterna, som framgår av artikel 58.2, är däremot mer omfattande. Som exempel kan nämnas att tillsynsmyndigheten enligt led g i den angivna artikeln får förelägga om radering av personuppgifter och att den enligt led i får påföra administrativa sanktionsavgifter. Vidare anges i artikel 58.3 vilken möjlighet myndigheten har att utfärda tillstånd och att ge råd.

Varje medlemsstat får enligt artikel 58.6 föreskriva att dess tillsynsmyndighet ska ha ytterligare befogenheter, utöver de som avses i punkterna 1, 2 och 3. Frågan om den svenska myndigheten bör ges sådana ytterligare befogenheter har övervägts av Utredningen om tillsynen över den personliga integriteten (Ju 2015:02). Utredningen konstaterar i sitt betänkande att det för närvarande inte finns något sådant behov (SOU 2016:65 s. 154–157). Betänkandet bereds för närvarande inom Regeringskansliet.

Bestämmelsen i artikel 58 om tillsynsmyndighetens befogenheter avser enligt dess ordalydelse endast tillsynen över tillämpningen av förordningens bestämmelser. Enligt regeringens bedömning torde dock dessa befogenheter omfatta tillsynen över tillämpningen av de nationella bestämmelser som kompletterar förordningen, på motsvarande sätt som

rätten till ersättning gäller vid överträdelser av sådana nationella bestämmelser, se avsnitt 17.1.1. Detta bör, som utredningen föreslår, framgå uttryckligen av dataskyddslagen. Befogenheterna bör gälla oavsett om de kompletterande nationella bestämmelserna har placerats i dataskyddslagen eller om de återfinns i sektorsspecifika författningar som rör behandling av personuppgifter. Eftersom dataskyddsförordningens tillämpningsområde utsträcks genom dataskyddslagen till att gälla även i verksamhet som inte omfattas av unionsrätten, kommer förordningens bestämmelser om tillsynsmyndighetens befogenheter som huvudregel att gälla även vid tillsyn i fråga om sektorsspecifika bestämmelser som kompletterar förordningen inom det utsträckta området.

Tillsynsmyndighetens befogenhet enligt artikel 58.2 i att ta ut administrativa sanktionsavgifter gäller vid sådana överträdelser som anges i artikel 83. Av den artikeln framgår att tillsynsmyndighetens befogenhet att ta ut sanktionsavgifter vid överträdelser av nationella bestämmelser är begränsad, på så sätt att den endast gäller i fråga om bestämmelser som har antagits på grundval av kapitel IX i dataskyddsförordningen. Med stöd av kapitel IX kan medlemsstaterna anta bestämmelser om t.ex. behandling av nationella identifikationsnummer (artikel 87) och behandling i anställningsförhållanden (artikel 88).

Avsikten med utredningens förslag i denna del är inte att utvidga möjligheterna att besluta om administrativa sanktionsavgifter jämfört med vad som gäller enligt dataskyddsförordningen (jfr SOU 2017:39 s. 377). En sådan utvidgning bör inte heller ske på generell nivå, genom en bestämmelse i dataskyddslagen. Regeringen anser att det av tydlighetsskäl uttryckligen bör framgå av dataskyddslagen att tillsynsmyndigheten inte får ta ut sanktionsavgifter vid andra överträdelser än de som avses i artikel 83 i dataskyddsförordningen. För att tillsynsmyndigheten ska kunna ta ut sanktionsavgifter i andra fall, krävs alltså en särskild reglering om detta, jfr avsnitt 16.2 och 16.3.3.

Regeringen anser till skillnad från *Förvaltningsrätten i Stockholm* att utpekandet av den myndighet som ska vara tillsynsmyndighet bör, liksom i dag, ske i en förordning och inte i dataskyddslagen, se avsnitt 14.1.2.

17.3.3 Kommunikation och delgivning

Regeringens bedömning: Bestämmelser om kommunikation inför och delgivning av beslut behövs inte i dataskyddslagen.

Utredningen föreslår till skillnad från regeringen särskilda bestämmelser om kommunikation inför och delgivning av beslut.

Remissinstanserna: Endast ett fåtal remissinstanser framför synpunkter på utredningens förslag i denna del. *Hovrätten för Västra Sverige* och *Kammarrätten i Göteborg* ifrågasätter behovet av särskilda bestämmelser om kommunikation.

Skälen för regeringens bedömning

Kommunikation

I 46 § PUL finns bestämmelser som utgör ytterligare processuella skyddsåtgärder för den personuppgiftsansvarige när tillsynsmyndigheten utövar sin befogenhet att besluta om vitesföreläggande. Bland annat anges att den personuppgiftsansvarige, enligt huvudregeln, ska ha fått tillfälle att yttra sig innan tillsynsmyndigheten beslutar om vite.

Utredningen föreslår att det i dataskyddslagen ska införas en liknande bestämmelse om kommunikation inför beslut som tillsynsmyndigheten avser att fatta med stöd av sina korrigerande tillsynsbefogenheter enligt artikel 58.2 i dataskyddsförordningen. Av 25 § i den nya förvaltningslagen framgår dock att innan en myndighet fattar ett beslut i ett ärende ska den, om det inte är uppenbart obehövligt, underrätta den som är part om allt material av betydelse för beslutet och ge parten tillfälle att inom en bestämd tid yttra sig över materialet. Denna bestämmelse fyller samma funktion som utredningens förslag.

I 25 § första stycket 2 och 3 i den nya förvaltningslagen finns visserligen undantag från kommunikationsplikten som saknar en direkt motsvarighet i utredningens förslag. Undantaget i punkten 2 – som gäller då det kan befaras att det annars skulle bli avsevärt svårare att genomföra beslutet – kommer dock knappast i fråga vid tillämpning av 58.2 i dataskyddsförordningen. När det gäller undantaget i punkten 3 – som gäller då ett väsentligt allmänt eller enskilt intresse kräver att beslutet meddelas omedelbart – aktualiseras endast vid tillfälliga beslut enligt artikel 58.2 f i förordningen. Sådana beslut skulle även enligt utredningens förslag kunna meddelas utan föregående kommunikation. Detta innebär, som *Hovrätten för Västra Sverige* och *Kammarrätten i Göteborg* påpekar, att den föreslagna bestämmelsen om kommunikation inte behövs. Regeringen lämnar därför inget sådant förslag.

Underrättelse om beslut

Enligt 46 § andra stycket PUL ska vitesföreläggande delges. Utredningen anser att den omständigheten att underlåtenhet att följa ett föreläggande enligt dataskyddsförordningen kan leda till sanktionsavgifter motiverar ett motsvarande krav på delgivning för alla typer av förelägganden som riktas mot en personuppgiftsansvarig eller ett personuppgiftsbiträde som tillsynsmyndigheten kan besluta enligt artikel 58.2 i förordningen.

Regeringen anser emellertid att detta inte utgör skäl för att frångå den generella principen om att en myndighet själv avgör på vilket sätt parterna ska underrättas om ett beslut (jfr 33 § tredje stycket i den nya förvaltningslagen). Det förtjänar dock att påpekas att formell delgivning kan behövas i vissa fall för att tillsynsmyndigheten i ett senare skede ska kunna visa att mottagaren tagit del av beslutet. Det kan t.ex. bli svårt att genom sanktionsavgift beivra en underlåtenhet att följa ett föreläggande, om föreläggandet inte har delgetts enligt delgivningslagen. Som framgår av avsnitt 16.4 anser regeringen att beslut om sanktionsavgifter alltid bör delges.

17.3.4 Platsundersökning ska inte kunna ske med tvång

Regeringens bedömning: Det bör inte införas några bestämmelser om tillsynsmyndighetens tillträde till personuppgiftsansvarigas eller personuppgiftsbiträdens lokaler.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Det stora flertalet remissinstanser instämmer i utredningens bedömning eller kommenterar den inte. *Kammarrätten i Göteborg* delar dock inte utredningens uppfattning och menar att dataskyddsförordningen kräver att bestämmelser införs som ger tillsynsmyndigheten möjlighet att tillgripa tvångsmedel. *Centrala studiestödsnämnden* anser att det bör klargöras om det föreligger en rätt för tillsynsmyndigheten att genomföra platsundersökningar med tvång även om det inte införs några särskilda nationella regler om detta.

Skälen för regeringens bedömning: Enligt dataskyddsförordningen ska tillsynsmyndigheten från den personuppgiftsansvarige och personuppgiftsbiträdet få tillgång till alla personuppgifter och all information som myndigheten behöver för att kunna fullgöra sina uppgifter (artikel 58.2 e). Tillsynsmyndigheten ska också få tillträde till alla lokaler som tillhör den personuppgiftsansvarige och personuppgiftsbiträdet, inbegripet tillgång till all utrustning och alla andra medel för behandling av personuppgifter (artikel 58.2 f). I skäl 129 till förordningen anges att undersökningsbefogenheten när det gäller tillträde till lokaler bör utövas i enlighet med särskilda krav i medlemsstaternas nationella processrätt, såsom kravet på att inhämta förhandstillstånd från rättsliga myndigheter.

Enligt 43 § c PUL har tillsynsmyndigheten rätt att få tillträde till sådana lokaler som har anknytning till behandlingen av personuppgifter. Tillsynsmyndigheten har dock inte möjlighet att tillgripa tvångsåtgärder. Befogenheten att få tillträde till lokalerna kan därmed sägas vara begränsad av den personuppgiftsansvariges eller biträdets samarbetsvilja, precis som tillgången till information. Vid genomförandet av dataskyddsdirektivet ansågs det olämpligt med regler som innebär att myndigheten skulle få genomdriva sina rättigheter med t.ex. polishjälp, eftersom det skulle kunna leda till ett större intrång i den personliga integriteten än det intrång som myndighetens tillsynsverksamhet syftar till att förebygga. Risken för att tillsynsmyndigheten skulle förbjuda fortsatt behandling av personuppgifter ansågs medföra att de personuppgiftsansvariga blir tillräckligt benägna att ge myndigheten det underlag den behöver (prop. 1997/98:44 s. 101–102).

Dataskyddsförordningen ger, i likhet med personuppgiftslagen, tillsynsmyndigheten en rätt att få tillträde till en personuppgiftsansvarigs eller ett personuppgiftsbiträdes lokaler. *Centrala studiestödsnämnden* efterfrågar ett klargörande om det föreligger en rätt att genomföra platsundersökningar med tvång även om det inte införs några särskilda nationella regler om detta. Regeringens bedömning är att så inte är fallet. Det kan dock konstateras att en undersökning av lokalerna i de allra flesta fall bör kunna ske med innehavarens medgivande. I vart fall torde risken för att tillsynsmyndigheten annars beslutar om tillfälligt förbud mot behandlingen, med stöd av artikel 58.2 f i dataskyddsförordningen, medföra att innehavaren ger tillsynsmyndigheten det tillträde den har rätt

till enligt artikel 58.1 f. Detta gäller i synnerhet då en underlåtelse att rätta sig efter ett föreläggande eller att ge tillsynsmyndigheten tillgång till uppgifter kan medföra att administrativa sanktionsavgifter tas ut enligt artikel 83.5 e. Av utredningen framgår att tvångsåtgärder hittills aldrig behövts och det finns inget skäl att anta att sådana kommer att behövas när dataskyddsförordningen börjar tillämpas.

I likhet med utredningen anser regeringen därför att det inte behövs några bestämmelser som ger tillsynsmyndigheten möjlighet att tillgripa tvångsåtgärder för att genomföra en platsundersökning. Till skillnad från *Kammarrätten i Göteborg* kan regeringen inte se att dataskyddsförordningen skulle kräva att sådana tvångsåtgärder införs.

17.3.5 Ansökan till domstol om tillsynsåtgärd

Regeringens förslag: Om tillsynsmyndigheten anser att det finns synnerliga skäl, får den ansöka hos förvaltningsrätten om att en tillsynsåtgärd ska vidtas, i stället för att själv besluta om åtgärden.

Utredningens förslag överensstämmer i sak med regeringens. Utredningen föreslår dock att ansökningsförfarandet ska vara tillämpligt om tillsynsmyndigheten vid handläggningen av ett ärende finner att det finns skäl att ifrågasätta giltigheten av en unionsrättsakt som påverkar tillämpningen av dataskyddsförordningen i ärendet.

Remissinstanserna: Det stora flertalet remissinstanser tillstyrker utredningens förslag eller har inga synpunkter på det. *Kammarrätten i Stockholm* anser att bestämmelsen utgör en helt ny företeelse i svensk rätt och att det behöver utvecklas hur förfarandet är tänkt att fungera. *Riksdagens ombudsmän* ifrågasätter behovet av ett särskilt förfarande och anser att utredningen föreslår ett nytt och för nationellt vidkommande främmande processuellt institut, vars konsekvenser inte har analyserats och belysts i tillräcklig utsträckning. *Förvaltningsrätten i Jönköping* och *Uppsala universitet* framför liknande invändningar. *Kammarrätten i Göteborg* noterar att den föreslagna bestämmelsen förefaller ha ett snävare tillämpningsområde än vad artikel 58.5 i dataskyddsförordningen ger uttryck för.

Skälen för regeringens förslag: Tillsynsmyndigheten ska enligt artikel 58.5 i dataskyddsförordningen ha befogenhet att bl.a. inleda eller på övrigt vis delta i rättsliga förfaranden, för att verkställa bestämmelserna i förordningen. En motsvarande bestämmelse finns i artikel 28.3 tredje strecksatsen i dataskyddsdirektivet, men berördes inte vid genomförandet av direktivet i svensk rätt.

EU-domstolen har, i det mål som gällde giltigheten av kommissionens beslut att de så kallade Safe Harbor-principerna säkerställde ett adekvat skydd för personuppgifter som överförs till USA, klargjort att bestämmelsen i dataskyddsdirektivet kan innebära ett krav på kompletterande processuella bestämmelser i nationell rätt (dom Schrems, C-362/14, EU:C:2015:650). I domen konstateras att EU-domstolen är exklusivt behörig att förklara en EU-rättsakt, såsom ett kommissionsbeslut om adekvat skyddsnivå i ett tredjeland, ogiltigt. Nationella domstolar har således inte någon sådan befogenhet, och än mindre de nationella

tillsynsmyndigheterna när de utreder om ett kommissionsbeslut är förenligt med skyddet för privatlivet och enskilda personers grundläggande fri- och rättigheter. EU-domstolen konstaterar mot den bakgrunden att om en nationell tillsynsmyndighet anser att det finns fog för en invändning mot behandling av personuppgifter, som har skett med stöd av ett kommissionsbeslut, måste tillsynsmyndigheten ha möjlighet att inleda ett rättsligt förfarande. Enligt EU-domstolen ankommer det på den nationella lagstiftaren att föreskriva rättsmedel som gör det möjligt för tillsynsmyndigheten att vid nationella domstolar göra gällande sådana invändningar. På så sätt kan den nationella domstolen, om den delar myndighetens tvivel angående en unionsrättsakts giltighet, hänskjuta en begäran om förhandsavgörande till EU-domstolen för att pröva rättsaktens giltighet.

I svensk rätt finns det ingen möjlighet för tillsynsmyndigheter att initiera en domstolsprövning i syfte att skapa förutsättningar för ett klargörande från EU-domstolen. Vissa remissinstanser, bl.a. *Riksdagens ombudsmän*, ifrågasätter om det finns behov av att införa en sådan möjlighet. Regeringen anser dock att det är svårt att tolka EU-domstolens dom på annat sätt. Det kan också konstateras att avsaknaden av en sådan möjlighet riskerar att medföra att överträdelser av dataskyddsregleringen inte kan beivras, eftersom tillsynsmyndigheten inte själv har befogenhet att underkänna en unionsrättsakt. En särskild ordning för denna, i och för sig ovanliga, situation bör därför införas, för att Sverige ska uppfylla kraven i artikel 58.5 i dataskyddsförordningen.

Om det finns skäl att ifrågasätta om en unionsrättsakt som påverkar tillämpningen av dataskyddsförordningen är giltig, t.ex. om ett kommissionsbeslut är förenligt med förordningen och fördragen, kan tillsynsmyndigheten inte själv fatta beslut om åtgärder enligt artikel 58.2 i dataskyddsförordningen, såsom att den personuppgiftsansvarige ska föreläggas att radera personuppgifter eller att behandling av personuppgifter ska förbjudas. Utredningen föreslår mot denna bakgrund att det ska införas en möjlighet för tillsynsmyndigheten att inleda ett förfarande vid allmän förvaltningsdomstol om den finner att det finns skäl att ifrågasätta giltigheten av en unionsrättsakt som påverkar tillämpningen av dataskyddsförordningen i ärendet.

Med anledning av vad bl.a. *Riksdagens ombudsmän* framför finns anledning att framhålla att utredningens förslag inte innebär en möjlighet för tillsynsmyndigheten att få till stånd en renodlad lagprövning i domstol. Det handlar i stället om ett ansökningsförfarande i ett konkret tillsynsärende där domstolen, i stället för tillsynsmyndigheten, som första instans fattar beslut i frågan om korrigerande tillsynsåtgärder ska vidtas eller inte. Om domstolen i ett sådant mål delar tillsynsmyndighetens tvivel angående giltigheten av den unionsrättsakt som förhindrar eller kräver att åtgärden vidtas, kan domstolen begära ett förhandsavgörande från EU-domstolen och därigenom få rättsaktens giltighet prövad innan något beslut om åtgärden fattas. Om domstolen däremot anser sig kunna besluta i sakfrågan utan att begära ett förhandsavgörande från EU-domstolen är den fri att göra det.

Denna typ av ansökningsförfarande hos domstol är inte någon ny företeelse, som bl.a. *Kammarrätten i Stockholm* menar, utan finns redan på

ett flertal tillsynsområden, bl.a. i 47 § PUL. Ansökningsförfarandet utgör därmed inte i sig något främmande element i svensk processrätt.

Utformningen av utredningens förslag innebär emellertid att ansökningsförfarandet är tillgängligt endast vid en normkonflikt. Detta kan leda till missuppfattningar om vad som ska prövas av domstolen. Som *Kammarrätten i Göteborg* påpekar, innebär en sådan avgränsning också att bestämmelsen får ett snävare tillämpningsområde än vad artikel 58.5 i dataskyddsförordningen kräver. Regeringen anser därför att det i bestämmelsen i stället ska anges att ansökningsförfarandet är tillgängligt om tillsynsmyndigheten anser att det finns synnerliga skäl. En sådan normkonflikt som beskrivs ovan utgör ett exempel på när synnerliga skäl föreligger. Tillsynsmyndighetens ansökan bör, i enlighet med utredningens förslag, göras hos den förvaltningsrätt som är behörig att pröva ett överklagande av tillsynsmyndighetens beslut. Prövningstillstånd bör krävas vid överklagande till kammarrätten.

17.4 Gemensamma tillsynsinsatser

17.4.1 Tilldelning av befogenheter enligt svensk rätt

Regeringens bedömning: Den svenska tillsynsmyndigheten får, i enlighet med gällande svensk rätt, förordna företrädare för en utländsk myndighet att agera för tillsynsmyndighetens räkning.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna instämmer i utredningens bedömning eller yttrar sig inte särskilt om denna.

Skälen för regeringens bedömning: Vid gränsöverskridande personuppgiftsbehandling kommer det att finnas flera behöriga tillsynsmyndigheter. Förordningen reglerar hur samarbetet mellan myndigheterna ska gå till i sådana situationer. Vid behov ska tillsynsmyndigheterna enligt artikel 62 genomföra gemensamma insatser. Enligt första meningen i artikel 62.3 får en tillsynsmyndighet tilldela befogenheter, även utredningsbefogenheter, till ledamöter eller personal från en annan medlemsstats tillsynsmyndighet som deltar i sådana gemensamma insatser. Bestämmelsen innebär att företrädare för en utländsk tillsynsmyndighet kan ges befogenhet att utöva offentlig makt i Sverige, i enlighet med den lagstiftning som gäller för den svenska tillsynsmyndigheten. Detta är enligt regeringens mening inte detsamma som att en förvaltningsuppgift överlåts till en utländsk tillsynsmyndighet. Av bestämmelsen framgår tvärtom tydligt att avsikten är att det är fysiska personer, ledamöter eller personal, som ska kunna tilldelas sådana befogenheter. Den svenska tillsynsmyndigheten kan således förordna företrädare för den andra myndigheten att utföra vissa uppgifter eller att inom ramen för vissa angivna befogenheter annars agera för tillsynsmyndighetens räkning. Enligt gällande svensk rätt är tillsynsmyndigheten fri att besluta om sådana förordnanden, även om det för anställning hade krävts svenskt medborgarskap. Några författningsåtgärder behövs därmed inte för att uppfylla denna del av bestämmelsen.

Enligt den sista meningen i artikel 62.3 ska den som tilldelas befogenheter omfattas av den medlemsstats nationella rätt som gäller för värdlandets tillsynsmyndighet. Det innebär bl.a. att företrädaren för en utländsk tillsynsmyndighet omfattas av offentlighets- och sekretesslagens bestämmelser om tystnadsplikt och att denne kan ställas till ansvar för eventuella tjänstefel.

17.4.2 Medgivande att utöva befogenheter enligt utländsk rätt

Regeringens bedömning: Det bör för närvarande inte införas något bemyndigande som gör det möjligt för tillsynsmyndigheten att medge företrädare för en utländsk tillsynsmyndighet att inom svenskt territorium agera enligt den medlemsstatens lagstiftning.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna instämmer i utredningens bedömning eller yttrar sig inte särskilt om denna. *Sveriges Radio AB* och *Sveriges Television AB* påpekar att det förekommer många journalistiska samarbeten över landsgränser och att det är av yttersta vikt att svenska journalister kan förlita sig på det svenska grundlagsskyddet och lagar som gäller för journalistisk verksamhet i övrigt i svensk rätt. Att ge utländska tillsynsmyndigheter rätt att agera enligt utländsk lagstiftning på svenskt territorium skulle enligt Sveriges Radio AB och Sveriges Television AB kunna innebära en ökad rättsosäkerhet.

Skälen för regeringens bedömning: Vid gemensamma tillsynsinsatser får tillsynsmyndigheten, enligt första meningen i artikel 62.3 i dataskyddsförordningen, medge företrädare för den deltagande myndigheten att utöva de utredningsbefogenheter som tilldelats dem enligt lagstiftningen i deras egen medlemsstat. I praktiken skulle ett sådant medgivande innebära att en utländsk tillsynsmyndighet får behörighet att agera på svenskt territorium i enlighet med utländsk lagstiftning. Medgivandet skulle därför enligt regeringens bedömning utgöra en överlåtelse av förvaltningsuppgift i regeringsformens mening. I bestämmelsen anges dock att medgivande får lämnas bara om lagstiftningen i värdlandet tillåter det. Tillsynsmyndigheterna har således inte direkt genom dataskyddsförordningen bemyndigats att medge andra medlemsstaters myndigheter rätt att utöva sina egna befogenheter inom värdlandets gränser. Det är i stället den nationella rätten i värdlandet som avgör om myndigheten överhuvudtaget kan vidta en sådan åtgärd.

En möjlighet för tillsynsmyndigheten att tillåta utländska myndighetsföreträdare att inom svenskt territorium utöva befogenheter enligt utländsk lagstiftning, bör enligt regeringens mening införas endast om det finns ett tydligt och uttalat behov som inte kan uppfyllas på något annat sätt. Något sådant behov har inte framkommit. Det bör därför, som utredningen konstaterar, vara tillräckligt att den utländska myndigheten får delta i insatserna i enlighet med dataskyddsförordningens direkt tillämpliga bestämmelser. Det kan noteras att lagstiftaren har gjort liknande bedömningar i andra ärenden rörande gränsöverskridande tillsyn (se t.ex. prop. 2012/13:4 s. 47 och prop. 2015/16:9 s. 191–192).

17.5 Överklagande av tillsynsmyndighetens beslut och av vissa beslut enligt dataskyddslagen

Regeringens förslag: Beslut i enskilda fall om behandling av personuppgifter som rör lagöverträdelser får överklagas till allmän förvaltningsdomstol. Detsamma gäller förvaltningsbeslut om behandling av personuppgifter för arkivändamål av allmänt intresse.

Tillsynsmyndighetens beslut enligt EU:s dataskyddsförordning och dess beslut om sanktionsavgifter enligt dataskyddslagen får överklagas till allmän förvaltningsdomstol. När ett beslut överklagas, är tillsynsmyndigheten motpart i domstolen.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Andra beslut enligt dataskyddslagen får inte överklagas.

Utredningens förslag överensstämmer i huvudsak med regeringens. I utredningens förslag anges inte uttryckligen att tillsynsmyndigheten har ställning som motpart i domstolen.

Remissinstanserna tillstyrker utredningens förslag eller har inga synpunkter på det.

Skälen för regeringens förslag

Överklagande av vissa beslut enligt dataskyddslagen

I avsnitt 11 föreslås att den myndighet som regeringen bestämmer ska ges befogenhet att i enskilda fall fatta beslut om att andra än myndigheter får behandla personuppgifter som rör lagöverträdelser. De förvaltningsbeslut som myndigheten meddelar med stöd av den föreslagna bestämmelsen bör kunna överklagas till allmän förvaltningsdomstol. Prövningstillstånd bör krävas vid överklagande till kammarrätten.

Vidare föreslås i avsnitt 14.1.2 att den myndighet som regeringen bestämmer ska ges befogenhet att i enskilda fall få fastställa rättslig grund för behandling av personuppgifter för arkivändamål av allmänt intresse. På motsvarande sätt föreslås att den myndighet som regeringen bestämmer ska få fatta beslut som tillåter behandling av känsliga personuppgifter för sådana ändamål. Även sådana förvaltningsbeslut bör kunna överklagas till allmän förvaltningsdomstol. Prövningstillstånd bör krävas vid överklagande till kammarrätten.

Överklagande av tillsynsmyndighetens beslut

Enligt artikel 78.1 i dataskyddsförordningen ska varje fysisk eller juridisk person ha rätt till ett effektivt rättsmedel mot ett rättsligt bindande beslut rörande dem som meddelats av en tillsynsmyndighet. I skäl 143 anges att denna rätt även avser beslut om att avvisa eller avslå ett klagomål, men däremot inte sådana åtgärder som inte är rättsligt bindande, såsom tillsynsmyndighetens yttranden eller rådgivning. Rätten till rättsmedel ska inte påverka något annat administrativt prövningsförfarande eller prövningsförfarande utanför domstol. Talan mot en tillsynsmyndighet ska enligt artikel 78.3 väckas vid domstolarna i den medlemsstat där tillsynsmyndigheten har sitt säte.

Rätten till ett effektivt rättsmedel mot myndighetsbeslut tillgodoses i svensk rätt normalt genom möjligheten att överklaga beslutet till allmän förvaltningsdomstol, dvs. till en förvaltningsrätt som första instans. När det gäller beslut som fattas enligt en EU-förordning följer rätten att överklaga av allmänna förvaltningsrättsliga principer. När den nya förvaltningslagen träder i kraft kommer rätten att överklaga att framgå av den lagen. Någon särskild överklagandebestämmelse behövs därmed i och för sig inte i dataskyddslagen när det gäller de beslut som tillsynsmyndigheten fattar enligt dataskyddsförordningen. Däremot behövs det, som regeringen anger i avsnitt 17.1.2, särskilda bestämmelser om rätten att överklaga vissa beslut som personuppgiftsansvariga myndigheter fattar enligt dataskyddsförordningen. Dessutom bör det i lagen föras in en bestämmelse om rätten att överklaga de beslut som tillsynsmyndigheten får meddela enligt dataskyddslagen, dvs. om att ta ut sanktionsavgifter av myndigheter eller vid överträdelser av artikel 10 samt, som framgår av föregående avsnitt, om överklagande av vissa andra beslut enligt lagen (jfr prop. 2017/18:180 s. 254). Mot bakgrund av den förhållandevis komplexa reglering om överklagande som behövs, och med hänsyn till det stora antalet beslutsfattande myndigheter och klagoberättigade parter, anser regeringen att regleringen om överklagande bör vara uttömmande i dataskyddslagen. Således bör även rätten att överklaga tillsynsmyndighetens beslut enligt dataskyddsförordningen uttryckligen anges i dataskyddslagen.

Sammanfattningsvis bör tillsynsmyndighetens beslut enligt dataskyddsförordningen få överklagas till allmän förvaltningsdomstol. Detsamma gäller tillsynsmyndighetens beslut enligt dataskyddslagen om sanktionsavgifter avseende myndigheter eller vid överträdelser av artikel 10 får överklagas till allmän förvaltningsdomstol. Andra beslut enligt dataskyddslagen än de i detta och föregående avsnitt nämnda, dvs. om sanktionsavgifter och om behandling av personuppgifter som rör lagöverträdelser eller om behandling av personuppgifter för arkivändamål av allmänt intresse, samt förvaltningsrättens beslut med anledning av tillsynsmyndighetens ansökan (avsnitt 17.3.5), bör inte kunna överklagas. Detta bör tydliggöras genom ett uttryckligt överklagandeförbud i lagen.

Enligt 42 § nya förvaltningslagen får ett beslut överklagas av den som beslutet angår, om det har gått honom eller henne emot. Ett beslut får enligt 41 § nya förvaltningslagen överklagas om beslutet kan antas påverka någons situation på ett inte obetydligt sätt. I 40 § samma lag anges att beslut överklagas till allmän förvaltningsdomstol och att prövningstillstånd krävs vid överklagande till kammarrätten.

Talerätt tillkommer alltså den som beslutet angår, om beslutet har gått denne emot. Den ordningen överensstämmer enligt regeringens bedömning med kravet på rättsmedel enligt artikel 78.1 i dataskyddsförordningen och bör således gälla även för beslut som tillsynsmyndigheten fattar enligt förordningen och dataskyddslagen. I praktiken innebär detta i normalfallet att det är den som beslutet riktas mot, oftast en personuppgiftsansvarig, ett personuppgiftsbiträde eller ett certifieringsorgan, som har rätt att överklaga. Det kan dock inte uteslutas att ett beslut skulle kunna ha rättsligt bindande följder även för andra än den som beslutet riktas mot. Dessa skulle i så fall också ha rätt att överklaga beslutet, enligt förvaltningslagens generella bestämmelse om talerätt.

Enligt svensk rättspraxis rörande personuppgiftslagen är Datainspektionens beslut att inte vidta någon åtgärd med anledning av en anmälan eller att avskriva ett tillsynsärende inte överklagbart (se RÅ 2010 ref. 29). I skäl 143 till dataskyddsförordningen anges dock att tillsynsmyndighetens beslut att avvisa eller avslå ett klagomål ska kunna angripas med ett effektivt rättsmedel. Den som berörs av ett sådant beslut är den enskilde som har lämnat in klagomålet. Vidare anges i artikel 77.2 att tillsynsmyndigheten ska underrätta den enskilde om hur arbetet fortskrider och vad resultatet blir, inbegripet möjligheten till rättslig prövning enligt artikel 78. EU-domstolen har angett att motsvarande bestämmelse i dataskyddsdirektivet (artikel 28.3) innebär att den person som har kommit in med en begäran till tillsynsmyndigheten ska ha tillgång till rättsmedel med vilka han eller hon vid nationella domstolar kan angripa det beslut som gått vederbörande emot (se t.ex. dom Schrems, C-362/14, EU:C:2015:650, punkt 64). Dessa omständigheter talar för att dataskyddsförordningen förutsätter att den enskilde ska ha en generell rätt att överklaga tillsynsmyndighetens beslut att t.ex. inte vidta någon åtgärd med anledning av ett klagomål.

Det finns emellertid också omständigheter som talar emot en sådan tolkning. Enligt artikel 78.1 är det den som beslutet rör som ska ha rätt till ett effektivt rättsmedel. Dessutom ska beslutet vara rättsligt bindande för denne. Ett beslut om att inte vidta några åtgärder med anledning av ett klagomål medför normalt inte några rättsligt bindande följder för den som har lämnat in klagomålet, även om det inte kan uteslutas att det någon gång skulle kunna förekomma, vilket i så fall skulle medföra överklagbarhet och ge talerätt enligt förvaltningslagen. Dessutom skulle en ovillkorlig rätt till domstolsprövning av ett sådant beslut kunna underminera tillsynsmyndighetens oberoende ställning, såsom denna kommer till uttryck i artikel 8.3 i EU:s stadga om de grundläggande rättigheterna och exempelvis artikel 52.1 i dataskyddsförordningen. Enligt artikel 57.1 f i dataskyddsförordningen ska tillsynsmyndigheten behandla klagomål och där så är lämpligt undersöka den sakfråga som klagomålet gäller. Tillsynsmyndigheten har därmed inte någon skyldighet att vidta tillsynsåtgärder eller ens att alltid närmare undersöka sakförhållandena. Tvärtom har tillsynsmyndigheten enligt dataskyddsförordningen, precis som enligt svensk tillsynstradition, ett tydligt utrymme att själv avgöra vilka tillsynsärenden som ska drivas och på vilket sätt det ska ske. Det framgår inte heller uttryckligen av förordningen att tillsynsmyndigheten måste fatta ett formellt beslut i varje klagomåls- eller tillsynsärende.

Sammanfattningsvis anser regeringen, i likhet med utredningen, att det är oklart om dataskyddsförordningen medför att den registrerade har rätt att överklaga tillsynsmyndighetens beslut att inte vidta någon åtgärd med anledning av ett klagomål. Oavsett hur förordningen ska tolkas i detta avseende, krävs det emellertid inte några författningsåtgärder i svensk rätt. Det bör i stället överlämnas till domstolarna att, genom en unionskonform tolkning av förvaltningslagens generella bestämmelser om överklagande, ta ställning i frågan.

Av dataskyddslagen bör det, som utredningen föreslår, framgå att tillsynsmyndighetens beslut enligt dataskyddsförordningen samt dess beslut om sanktionsavgifter enligt dataskyddslagen får överklagas till

allmän förvaltningsdomstol. Av tydlighetsskäl bör det även framgå av bestämmelsen att tillsynsmyndigheten har ställning som motpart i ett sådant mål hos domstolen (jfr 22 kap. 5 § lagen om offentlig upphandling). Vidare bör det anges att prövningstillstånd krävs vid överklagande till kammarrätten. Formerna för överklagande av tillsynsmyndighetens beslut, vilken överklagandefrist som ska gälla, vem som har talerätt m.m., bör inte avvika från förvaltningslagens bestämmelser. Regeringen föreslår därför inga särskilda bestämmelser om detta.

17.6 Ideella organisationer som är verksamma inom dataskyddsområdet

Regeringens bedömning: Endast fysiska personer får agera ombud, men uppdraget att föra den registrerades talan kan ges till en eller flera företrädare för en organisation. Ideella organisationer bör för närvarande inte ges rätt att föra talan i ärenden och mål om behandling av personuppgifter.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Det stora flertalet remissinstanser instämmer i utredningens bedömning eller kommenterar den inte. *Sveriges Television AB* påpekar att de registrerade som önskar biträde av en ideell organisation inte på något sätt är förhindrade från att anlita organisationen i fråga, varför den föreslagna lösningen varken stärker eller försvagar skyddet för deras rättigheter. *Förvaltningsrätten i Stockholm*, som också instämmer i utredningens bedömning, efterlyser dock ytterligare klargörande uttalanden om hur domstolarna förväntas agera. *Kammarrätten i Göteborg* anser att den möjlighet som enligt gällande rätt finns att ge fullmakt åt en företrädare för en organisation inte uppfyller de krav förordningen ställer. *Dataskydd.net* är kritiskt mot att utredningen inte gjort någon ansats att förenkla grupptalan.

Skälen för regeringens bedömning

Förordningens reglering

Dataskyddsförordningen innehåller bestämmelser som tar sikte på organ, organisationer eller sammanslutningar som

- bedrivs utan vinstsyfte,
- är inrättade i enlighet med lagen i en medlemsstat,
- vars stadgeenliga mål är av allmänt intresse, och
- är verksamma inom området skydd av registrerades rättigheter och friheter när det gäller skyddet av deras personuppgifter.

Enligt artikel 80.1 ska den registrerade ha rätt att ge en sådan organisation i uppdrag att för hans eller hennes räkning lämna in ett klagomål till tillsynsmyndigheten och att utöva rätten till effektiva rättsmedel. Den registrerade ska också, om så föreskrivs i medlemsstatens nationella rätt, ha rätt att ge den ideella organisationen i uppdrag att för hans eller hennes räkning utöva rätten till ersättning.

I artikel 80.2 anges att medlemsstaterna får föreskriva att en ideell organisation, oberoende av en registrerads mandat, har rätt att ge in klagomål till tillsynsmyndigheten och utöva de rättigheter som avses i artiklarna 78 och 79. Organisationer får däremot inte ges rätt att kräva ersättning på en registrerad persons vägnar utan den registrerades mandat.

Ideella organisationer som ombud för den registrerade

En juridisk person kan enligt gällande svensk rätt inte företräda en enskild i domstol. En ideell organisation kan således inte vara ombud för den registrerade i ett förvaltningsmål eller i ett skadeståndsmål i allmän domstol. Bestämmelserna om rättegångsombud i 12 kap. rättegångsbalken utgår nämligen från förutsättningen att ombudet är en fysisk person. En ideell organisation skulle därmed sannolikt avvisas som ombud i ett skadeståndsmål i allmän domstol. Detsamma gäller sedan den 1 juli 2013 även i mål i allmän förvaltningsdomstol. Bestämmelser om ombud finns bl.a. i 48 och 49 §§ förvaltningsprocesslagen (1971:291) och av förarbetena till den nuvarande lydelsen framgår att det inte längre kommer att vara möjligt att i allmän förvaltningsdomstol använda sig av juridiska personer som ombud eller biträden (prop. 2012/13:45 s. 106–107).

När den nya förvaltningslagen träder i kraft den 1 juli 2018 kommer en juridisk person inte heller att kunna agera ombud i förvaltningsärenden. Detta följer av 14 § i den nya lagen. Den registrerade kan därmed inte ge en ideell organisation i uppdrag att för hans eller hennes räkning lämna in klagomål till tillsynsmyndigheten. Detsamma gäller vid utövande av rätten att hos Justitiekanslern begära skadestånd, när en personuppgiftsansvarig statlig myndighet har orsakat den enskilde skada genom överträdelser av dataskyddsförordningen.

Ett rättegångsombud ska enligt 12 kap. 2 § rättegångsbalken vara lämplig med hänsyn till redbarhet, insikter och tidigare verksamhet. I 48 § förvaltningsprocesslagen och 14 § nya förvaltningslagen anges endast att ombudet ska vara lämpligt för uppdraget. Det finns varken i rättegångsbalken eller i förvaltningsprocesslagen, eller i den nya förvaltningslagen, något krav på att ombudet ska vara advokat eller jurist. Den företrädare för den ideella organisationen som skulle ha fört talan om organisationen själv hade godkänts som ombud kommer därmed normalt att kunna godkännas som ombud för den registrerade (jfr prop. 2002/03:65 s. 167).

Regeringen anser i likhet med utredningen att ett uppdrag som ombud eller biträde bör vara ett personligt uppdrags- och ansvarsförhållande. Även om en ideell organisation skulle få anlitas som ombud skulle det i realiteten vara en fysisk person som för den enskildes talan. Fullmakten till organisationen kan därmed utan olägenhet utformas så att den också omfattar den eller de fysiska personer som faktiskt utför uppdraget. Mot denna bakgrund anser regeringen, till skillnad från *Kammarrätten i Göteborg*, att den gällande ordningen är förenlig med dataskyddsförordningen och att det saknas skäl att föreslå några bestämmelser som i detta avseende avviker från rättegångsbalken, förvaltningsprocesslagen och den nya förvaltningslagen.

Ideella organisationer ska inte ges talerätt

Medlemsstaterna får enligt dataskyddsförordningen meddela nationella föreskrifter som ger ideella organisationer en självständig talerätt avseende registrerades rättigheter. En sådan talerätt skulle ge dessa organisationer möjlighet att utan den registrerades mandat t.ex. ge in klagomål till tillsynsmyndigheten, om organisationen anser att den registrerades rättigheter har kränkts.

En liknande ordning gäller enligt svensk rätt i fråga om kränkningar i form av diskriminering. Enligt 6 kap. 2 § diskrimineringslagen får en ideell förening som enligt sina stadgar har att ta till vara sina medlemmars intressen och som inte är en arbetstagarorganisation, som part föra talan om diskriminering. En förutsättning är dock att den enskilde medger detta. Ett annat exempel som kan nämnas är möjligheten till organisationstalan enligt lagen (2002:599) om grupprättegång. I 5 § i den lagen anges att organisationstalan får väckas av en ideell förening som i enlighet med sina stadgar tillvaratar konsument- eller löntagarintressen i tvister mellan konsumenter och en näringsidkare om någon vara, tjänst eller annan nyttighet som näringsidkaren erbjuder till konsumenter.

När det gäller skyddet för den personliga integriteten har det under senare år blivit vanligare med ideella organisationer som är verksamma inom dataskyddsområdet. I Sverige är dock denna typ av verksamhet än så länge liten. För närvarande anser regeringen, i likhet med utredningen, att det inte finns skäl att på detta område införa särskilda bestämmelser om talerätt för ideella organisationer. Beroende på hur den ideella sektorn utvecklas är det dock inte uteslutet att det i framtiden kan komma att finnas skäl att återkomma till denna fråga.

17.7 Parallella domstolsförfaranden

Regeringens bedömning: En svensk domstol kan förklara ett mål vilande, om ett förfarande rörande samma sakfråga pågår i en domstol i en annan medlemsstat. Däremot kan domstolen enligt svensk rätt inte förklara sig obehörig att handlägga målet.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: *Kammarrätten i Göteborg* anser att det kan behövas kompletterande svenska bestämmelser på detta område. *Förvaltningsrätten i Stockholm* anser att förordningen med direkt effekt ger domstolarna en möjlighet att i ett enskilt fall förklara sig obehörig. Övriga remissinstanser framför inga invändningar mot utredningens bedömning i denna del.

Skälen för regeringens bedömning: Om en behörig domstol i en medlemsstat har information om att ett förfarande pågår i en domstol i en annan medlemsstat rörande samma sakfråga och samma personuppgiftsansvarig eller personuppgiftsbiträde, ska den förstnämnda domstolen enligt artikel 81.1 i dataskyddsförordningen kontakta den andra domstolen för att få det bekräftat. I artikel 81.2 anges att om förfaranden som rör samma sakfråga och samma personuppgiftsansvarig eller personuppgiftsbiträde pågår i en domstol i en annan medlemsstat, får alla andra

behöriga domstolar än den där förfarandet först inleddes vilandeförklara förfarandena. Om ett förfarande prövas i första instans får domstolen, utom den domstol vid vilken förfarandena först inleddes, enligt artikel 81.3 förklara sig obehörig på begäran av en av parterna. Detta gäller under förutsättningen att den domstol vid vilken förfarandet först inleddes är behörig att pröva de berörda förfarandena och dess lagstiftning tillåter förening av dessa.

I skäl 144 till förordningen anges att förfarandena ska anses vara relaterade, om de är så nära förenade att en gemensam handläggning och dom är påkallad för att undvika att oförenliga domar meddelas.

I 32 kap. 5 § rättegångsbalken finns en bestämmelse som innebär att rätten får förklara ett mål vilande, om det för prövning av målet är av synnerlig vikt att en fråga som är föremål för annan rättegång eller behandling i annan ordning först avgörs. Någon motsvarighet till denna bestämmelse finns inte i förvaltningsprocesslagen. Det innebär dock inte att förvaltningsdomstolar är förhindrade att förklara ett mål vilande av motsvarande skäl. Vid införandet av förvaltningsprocesslagen ansågs detta tvärtom så självklart att lagtexten inte behövde belastas med någon hänvisning till rättegångsbalken (prop. 1971:30 del 2 s. 600). Möjligheten till vilandeförklaring har inte bara utnyttjats när flera relaterade mål förekommit i samma domstol eller i olika svenska domstolar, utan har också använts för att invänta EU-domstolens dom i ett annat mål avseende en för målet central rättsfråga (se t.ex. RÅ 2005 ref. 33 och Kammarrätten i Stockholms dom den 22 augusti 2014 i mål nr 1724-13).

Sedan den 1 juli 2013 får Högsta förvaltningsdomstolen enligt 36 a § förvaltningsprocesslagen meddela prövningstillstånd som begränsas till att gälla en viss fråga eller en viss del av målet. I avvaktan på att prövning sker i enlighet med ett sådant begränsat prövningstillstånd får Högsta förvaltningsdomstolen förklara frågan om meddelande av prövningstillstånd rörande målet i övrigt helt eller delvis vilande. Med anledning av ett påpekande under remissbehandlingen från Högsta förvaltningsdomstolens ledamöter underströks i förarbetena att den omständigheten att denna typ av vilandeförklaring numera uttryckligen regleras i förvaltningsprocesslagen inte inskränker allmän förvaltningsdomstols möjligheter att även i andra sammanhang vilandeförklara mål (prop. 2012/13:45 s. 139).

Mot bakgrund av att förvaltningsdomstolarna redan på grundval av förvaltningsprocessrättsliga principer och praxis kan förklara mål vilande när ett mål rörande samma sakfråga pågår i en annan domstol, även en utländsk sådan, finns det inte skäl att införa några särskilda bestämmelser i svensk rätt med anledning av artikel 81.2 i dataskyddsförordningen. Hur sådana situationer ska hanteras i praktiken får lämnas till domstolarna att avgöra.

Möjligheten för en domstol att förklara sig obehörig på begäran av en av parterna, enligt artikel 81.3, förutsätter dels att den domstol där förfarandet först inleddes är behörig att göra prövningen, dels att dess lagstiftning tillåter förening av förfarandena.

Enligt 7 § förvaltningsprocesslagen kan ett mål överlämnas till en annan domstol om domstolen finner att den saknar behörighet att handlägga målet men att en annan motsvarande domstol skulle vara behörig. Vidare följer det av 8 a och 14 §§ lagen (1971:289) om allmänna

förvaltningsdomstolar att mål under vissa omständigheter kan överlämnas, om det vid mer än en förvaltningsrätt eller kammarrätt förekommer mål som har nära samband med varandra. Det finns däremot för närvarande inte några bestämmelser i svensk förvaltningsprocessrätt som möjliggör för en domstol att förklara sig obehörig att handlägga ett mål på den grunden att det vid en utländsk domstol förekommer ett mål som rör samma sakfråga. I artikel 81.3 i dataskyddsförordningen anges dock endast att domstolen får förklara sig obehörig. Till skillnad från *Kammarrätten i Göteborg* instämmer därför regeringen i utredningens bedömning att förordningen i detta avseende inte är tvingande och att det därmed inte finns någon skyldighet för medlemsstaterna att införa processrättsliga bestämmelser som möjliggör ett sådant överlämnade. Regeringen ser heller inte något annat skäl till att införa en sådan ordning. Huruvida bestämmelsen i dataskyddsförordningen ger domstolarna en möjlighet att utan stöd av nationella bestämmelser förklara sig obehörig, som *Förvaltningsrätten i Stockholm* menar, överlämnas till domstolarna att bedöma.

18 Ikraftträdande- och övergångsbestämmelser

Regeringens förslag: Dataskyddslagen träder i kraft den 25 maj 2018.

Genom lagen upphävs personuppgiftslagen.

I stället för vad som sägs i den bestämmelse i dataskyddslagen som utsträcker dataskyddsförordningens tillämpningsområde, ska personuppgiftslagen fortsätta att gälla i sådan verksamhet hos Försvarsmakten, Försvarets radioanstalt och Totalförsvarets rekryteringsmyndighet som inte omfattas av unionsrätten.

Personuppgiftslagen gäller fortfarande vid behandling av personuppgifter som utförs av behöriga myndigheter i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, i vilket även ingår att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten.

Personuppgiftslagen gäller fortfarande i den utsträckning som det i en annan lag eller en förordning finns bestämmelser som innehåller hänvisningar till den.

Personuppgiftslagen gäller fortfarande för överklagande av beslut som har meddelats med stöd av den lagen.

Personuppgiftslagens straffbestämmelse gäller fortfarande för överträdelser som har skett före ikraftträdandet.

Sådana beslut i enskilda fall avseende behandling av personuppgifter som rör lagöverträdelser och som har meddelats med stöd av personuppgiftslagen gäller fortfarande.

Utredningens förslag överensstämmer delvis med regeringens. Utredningen föreslår inte några särskilda bestämmelser av övergångskaraktär för sådan verksamhet hos försvarsmyndigheterna som inte omfattas av

unionsrätten eller för behöriga myndigheter som omfattas av det nya dataskyddsdirektivet. Utredningen föreslår inte heller någon övergångsbestämmelse rörande beslut i enskilda fall avseende behandling av personuppgifter som rör lagöverträdelser. Däremot föreslår utredningen att personuppgiftslagen fortfarande ska gälla för ärenden hos Datainspektionen som har inletts men inte avgjorts före ikraftträdandet samt i fråga om skadestånd för skada som har orsakats före ikraftträdandet.

Remissinstanserna: Det stora flertalet remissinstanser tillstyrker utredningens förslag eller har inga synpunkter på det. *Hovrätten för Västra Sverige*, *Förvaltningsrätten i Malmö*, *Datainspektionen*, *Pensionsmyndigheten*, *Länsstyrelsen i Kronobergs län*, *Länsstyrelsen i Skåne*, *Länsstyrelsen i Östergötlands län*, *Centrala studiestödsnämnden* och *Bolagsverket* invänder mot utredningens förslag att personuppgiftslagen ska fortsätta gälla i den utsträckning som det i en annan lag eller förordning finns bestämmelser som innehåller hänvisningar till den lagen (punkt 3 i utredningens förslag) samt påpekar att dataskyddsförordningen ska tillämpas från och med den 25 maj 2018. Hovrätten för Västra Sverige anser att övergångsbestämmelsen bör ange att bestämmelserna i dataskyddsförordningen ska tillämpas i stället för bestämmelserna i personuppgiftslagen. Pensionsmyndigheten föreslår att övergångsbestämmelsen ska ange att personuppgiftslagen ska tillämpas så länge dess bestämmelser inte står i strid med förordningen. Länsstyrelsen i Skåne anser att det i vart fall ska införas en slutlig gräns för hur länge personuppgiftslagen ska fortsätta att tillämpas. *Försäkringskassan* och *Göteborgs universitet* efterfrågar ett resonemang kring eventuella normkonflikter som skulle kunna uppstå om personuppgiftslagen fortsätter att gälla. Datainspektionen invänder mot förslaget att personuppgiftslagen ska gälla för ärenden hos Datainspektionen som har inletts men inte avgjorts före ikraftträdandet (punkt 4 i utredningens förslag) och anser att dataskyddsförordningen ska tillämpas även om ärendet inletts före den 25 maj 2018. Datainspektionen invänder även mot förslaget att äldre föreskrifter ska gälla för överträdelser som skett före ikraftträdandet (punkt 7 i utredningens förslag) och menar att utredningen inte visat att det i detta fall är möjligt att frångå gällande bestämmelser rörande principen om lindrigaste lag. Förvaltningsrätten i Malmö invänder mot uttrycket äldre föreskrifter och påpekar att detta även skulle kunna omfatta exempelvis registerförfattningar (punkterna 4–7 i utredningens förslag). *Försvarsmakten* anser att det bör införas ytterligare en övergångsbestämmelse som innebär att personuppgiftslagen fortsatt ska gälla för de delar av Försvarsmaktens verksamhet som är av betydelse för Sveriges säkerhet. *Försvarets radioanstalt* anser att det bör införas en övergångsbestämmelse som innebär att personuppgiftslagen ska fortsätta att gälla för myndighetens informationssäkerhetsverksamhet. *Svensk Försäkring* anser att en övergångsbestämmelse bör övervägas som klargör att nu gällande tillstånd att behandla personuppgifter som rör lagöverträdelser gäller även fortsättningsvis.

Skälen för regeringens förslag

Ikraftträdande

Av artikel 99 i dataskyddsförordningen följer att förordningen trädde i kraft den 25 maj 2016. Förordningen ska enligt samma artikel tillämpas från och med den 25 maj 2018. Av skäl 171 framgår att pågående behandling bör ha bringats i överensstämmelse med förordningen under denna tvåårsperiod.

Dataskyddslagen bör träda i kraft den dag dataskyddsförordningen börjar tillämpas, dvs. den 25 maj 2018. Samtidigt bör personuppgiftslagen upphöra att gälla (jfr avsnitt 5.1).

Viss verksamhet som inte omfattas av unionsrätten

Dataskyddsförordningen ska enligt artikel 2.2 a inte tillämpas vid behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av unionsrätten, t.ex. i verksamhet som rör nationell säkerhet. I avsnitt 6.1 föreslår regeringen emellertid att förordningen, i tillämpliga delar, och dataskyddslagen ska gälla även i sådan verksamhet. Detta ska dock inte gälla i verksamhet som omfattas av bl.a. lagen om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst samt lagen om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet. Båda dessa författningar är för närvarande föremål för översyn av en särskild utredare (dir. 2017:42). Utredaren ska enligt kommittédirektiven bl.a. analysera vilket utrymme det finns för nationell reglering av den personuppgiftsbehandling i Försvarsmakten och Försvarets radioanstalt som i dag regleras i personuppgiftslagen, och utifrån den analysen bedöma om behandlingen helt eller delvis bör regleras särskilt.

Viss behandling av personuppgifter som sker hos Totalförsvarets rekryteringsmyndighet regleras av lagen (1998:938) respektive förordningen (1998:1229) om behandling av personuppgifter om totalförsvarspliktiga. Även dessa författningar är för närvarande föremål för översyn av en särskild utredare. I utredarens uppdrag ingår att analysera om fler personalkategorier än de totalförsvarspliktiga ska ingå i särlagstiftningen samt att överväga om annan personuppgiftsbehandling som förekommer hos myndigheten bör omfattas av den nya regleringen (dir. 2016:103).

De aktuella författningarna reglerar bara vissa delar av den behandling av personuppgifter som sker hos Försvarsmakten, Försvarets radioanstalt och Totalförsvarets rekryteringsmyndighet. I övrigt gäller personuppgiftslagen. Som framgår ovan kan dock det pågående utredningsarbetet komma att leda till att författningarnas tillämpningsområden utvidgas till att även avse viss behandling som i dag regleras av personuppgiftslagen. Mot den bakgrunden anser regeringen, i likhet med *Försvarsmakten* och *Försvarets radioanstalt*, att det behövs en särskild reglering som medför att personuppgiftslagen fortsätter att gälla, i stället för dataskyddsförordningen och dataskyddslagen, i sådan verksamhet hos Försvarsmakten, Försvarets radioanstalt och Totalförsvarets rekryteringsmyndighet som inte omfattas av unionsrätten. Vid behandling av personuppgifter som sker i verksamhet som omfattas av unionsrätten är dock

dataskyddsförordningen direkt tillämplig fr.o.m. den 25 maj 2018 även hos dessa myndigheter.

Förslag till övergångsbestämmelser som i sak överensstämmer med regeringens förslag har beretts med *Säkerhetspolisen*, *Datainspektionen*, *Säkerhets- och integritetsskyddsnämnden*, Försvarsmakten, Försvarets radioanstalt, *Totalförsvarets rekryteringsmyndighet* och *Myndigheten för samhällsskydd och beredskap*, som inte framför några invändningar.

Mot bakgrund av det anförda bör det införas en bestämmelse som anger att, i stället för vad som sägs i den bestämmelse i dataskyddslagen som utsträcker dataskyddsförordningens tillämpningsområde, ska personuppgiftslagen fortsätta att gälla i sådan verksamhet hos Försvarsmakten, Försvarets radioanstalt och Totalförsvarets rekryteringsmyndighet som inte omfattas av unionsrätten. Bestämmelsen är av övergångskaraktär och ska upphävas i samband med att den anpassade regleringen om behandling av personuppgifter i dessa myndigheters verksamhet träder i kraft.

Verksamhet som omfattas av det nya dataskyddsdirektivet

Dataskyddsförordningen ska enligt artikel 2.2 d inte tillämpas på behandling av personuppgifter som behöriga myndigheter utför i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, i vilket även ingår att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten. Sådan behandling omfattas i stället av det nya dataskyddsdirektivet, som ska vara genomfört i nationell rätt senast den 6 maj 2018.

Arbetet med att anpassa svensk lagstiftning till den nya EU-regleringen är mycket omfattande och delvis mycket komplicerat. Detta gäller i hög grad genomförandet av det nya dataskyddsdirektivet, som i huvudsak ska ske genom införandet av en ny ramlag, brottsdatalagen. Denna ramlag ska kompletteras genom anpassningar i de brottsbekämpande myndigheternas registerförfattningar. Regeringen kan konstatera att all den lagstiftning som ska genomföra direktivet inte kommer att träda i kraft i tid. För de behöriga myndigheter som i dag har en registerförfattning bör detta inte utgöra något praktiskt problem, eftersom de nuvarande författningarna till stor del uppfyller de nya kraven (se även följande avsnitt om författningar som hänvisar till personuppgiftslagen). För de behöriga myndigheter som inte omfattas av någon registerförfattning, kommer det däremot inte att finnas någon tillämplig dataskyddsreglering då personuppgiftslagen upphävs, eftersom dessa myndigheter enligt artikel 2.2 d i dataskyddsförordningen inte ska tillämpa förordningen. Mot den bakgrunden anser regeringen, i likhet med vad som anförs av Utredningen om 2016 års dataskyddsdirektiv, SOU 2017:29 s. 655–657, att det behövs en övergångsreglering som ger rättsligt stöd för personuppgiftsbehandling på direktivets område under den tid som lagstiftningsarbetet med en ny ramlag på direktivets område pågår. Några invändningar mot Utredningen om 2016 års dataskyddsdirektivs bedömning i denna del har inte framförts vid remissbehandlingen av betänkandet (Ju2017/03283/L4). Det bör därför införas en bestämmelse som anger att personuppgiftslagen fortfarande gäller för sådan behandling av personuppgifter som avses i artikel 2.2 d i EU:s dataskyddsförordning, i

den ursprungliga lydelsen. Bestämmelsen, som är av övergångskaraktär, ska sedan upphävas i samband med att den nya ramlagen träder i kraft.

Hänvisningar till personuppgiftslagen

Hänvisningar till personuppgiftslagen förekommer i ett stort antal författningar. Eftersom dataskyddsförordningen är direkt tillämplig från och med den 25 maj 2018 och personuppgiftslagen samtidigt kommer att upphävas är det naturligtvis angeläget att dessa författningar så snart som möjligt ändras och anpassas till förordningen. Alltsedan förordningen antogs har det därför pågått ett intensivt arbete, i en rad utredningar och inom samtliga departement, med att analysera vilka ändringar i lagar och förordningar som behövs eller är lämpliga med anledning av dataskyddsförordningen. Parallellt med detta pågår arbetet med att genomföra det nya dataskyddsdirektivet. Arbetet med att anpassa svensk lagstiftning till den nya EU-regleringen är mycket omfattande och delvis mycket komplicerat. Regeringen kan nu konstatera att detta arbete inte kommer att vara helt avslutat den 25 maj 2018. När personuppgiftslagen upphör att gälla kommer det således fortfarande att finnas ett antal författningar med hänvisningar till personuppgiftslagen som ännu inte har hunnit ändras.

I huvudsak förekommer det två olika slag av så kallade registerförfattningar. Det vanligaste är att sådana författningar gäller *utöver* personuppgiftslagen, vilket innebär att personuppgiftslagen gäller om inte annat anges i den särskilda författningen. Det finns dock även registerförfattningar som gäller *i stället för* personuppgiftslagen. I båda dessa fall innehåller författningarna hänvisningar till personuppgiftslagen eller till vissa bestämmelser i denna.

Således anges t.ex. i studiestödsdatalagen att personuppgiftslagen tillämpas vid behandling av personuppgifter i Centrala studiestödsnämndens studiestödsverksamhet, i den mån den lagen innehåller bestämmelser om behandling av personuppgifter som saknar motsvarighet i studiestödsdatalagen. I patientdatalagen anges på motsvarande sätt att personuppgiftslagen gäller om inte annat följer av patientdatalagen eller föreskrifter som meddelats med stöd av den lagen. Utlänningsdatalagen (2016:27) och polisdatalagen utgör däremot exempel på författningar som gäller i stället för personuppgiftslagen. Enligt dessa författningar ska endast vissa särskilt angivna bestämmelser i personuppgiftslagen tillämpas. Det finns också författningar om behandling av personuppgifter som är heltäckande och därmed fristående från personuppgiftslagen. Lagen om behandling av personuppgifter inom Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst och lagen om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet är exempel på sådana författningar.

Författningar som hänvisar till personuppgiftslagen innehåller bestämmelser som specificerar, kompletterar eller gör undantag från personuppgiftslagen. När dataskyddsförordningen börjar tillämpas kommer dessa bestämmelser i praktiken i stället att utgöra kompletterande bestämmelser till förordningen. Eftersom vissa författningar som hänvisar till personuppgiftslagen inte kommer att hinna ändras innan data-

skyddsförordningen ska börja tillämpas, kommer sådana författningar fortfarande att hänvisa till personuppgiftslagen vid denna tidpunkt. Det finns ett behov av att klargöra hur sådana hänvisningar ska tolkas, eftersom det annars kan uppstå tillämpningsproblem. I värsta fall skulle författningar med hänvisningar till personuppgiftslagen kunna tolkas som att personuppgiftsbehandlingen delvis är oreglerad, med brister i integritetsskyddet som följd. Regeringen delar därför utredningens bedömning om att det behövs någon form av övergångsreglering.

Utredningen föreslår att personuppgiftslagen ska fortsätta gälla i den utsträckning som det i en annan lag eller förordning finns bestämmelser som innehåller hänvisningar till den lagen. Denna typ av övergångsbestämmelse används även i den nya förvaltningslagen. Några remissinstanser, bl.a. *Hovrätten för Västra Sverige*, *Datainspektionen och Pensionsmyndigheten*, invänder mot utredningens förslag och påpekar att dataskyddsförordningen ska tillämpas från och med den 25 maj 2018. Ett par remissinstanser, bl.a. *Göteborgs universitet*, förutser normkonflikter.

Regeringen kan dock konstatera att de sektorsspecifika författningarna som det nu är fråga om i princip uteslutande avser sådan behandling av personuppgifter som utförs på grundval av rättsliga förpliktelser, uppgifter av allmänt intresse eller som ett led i myndighetsutövning. På dessa områden har medlemsstaterna enligt dataskyddsförordningen i stort sett samma utrymme att införa eller behålla nationella bestämmelser om behandlingen som enligt dataskyddsdirektivet. Bestämmelserna i personuppgiftslagen som de sektorsspecifika författningarna hänvisar till motsvaras också i allt väsentligt av bestämmelser i dataskyddsförordningen. Mot denna bakgrund bedömer regeringen att risken är mycket liten för att normkonflikter ska uppstå under den korta tid som övergångsbestämmelsen behövs. Däremot finns det i dataskyddsförordningen bestämmelser som saknar motsvarighet i personuppgiftslagen, t.ex. rörande anmälan av personuppgiftsincidenter, krav på konsekvensbedömning och sanktionsavgifter. Dessa bestämmelser ska givetvis tillämpas från och med den 25 maj 2018, även om behandlingen också omfattas av bestämmelser i en registerförfattning som hänvisar till personuppgiftslagen. Någon normkonflikt uppstår inte heller i dessa avseenden. Det finns mot denna bakgrund inte skäl att, som Pensionsmyndigheten föreslår, uttryckligen ange i övergångsbestämmelsen att personuppgiftslagen ska tillämpas endast så länge dess bestämmelser inte står i strid med förordningen.

Regeringen har övervägt om övergångsbestämmelsen bör utformas på det sätt som Hovrätten för Västra Sverige förordar, dvs. att bestämmelserna i dataskyddsförordningen ska tillämpas i stället för de bestämmelser i personuppgiftslagen som en viss hänvisning avser. Regeringen anser emellertid att den typen av bestämmelser bör undvikas (Gröna boken – Riktlinjer för författningsskrivning, Ds 2014:1 s. 111–112). Vidare anser regeringen att det saknas skäl att tidsbegränsa övergångsbestämmelsens giltighet, som *Länsstyrelsen i Skåne* föreslår, eftersom denna med automatik kommer att sakna betydelse när samtliga författningar som innehåller hänvisningar till personuppgiftslagen har ändrats.

Sammanfattningsvis anser regeringen således, i likhet med utredningen, att det bör införas en övergångsbestämmelse som anger att personuppgiftslagen fortfarande gäller i den utsträckning som det i en

annan lag eller en förordning finns bestämmelser som innehåller hänvisningar till den lagen.

Ärendehandläggning och överklagande av beslut

En utgångspunkt i förordningen är som nämns ovan att behandling som pågår den dag då förordningen börjar tillämpas ska ha bringats i överensstämmelse med förordningen. Personuppgiftsansvariga och personuppgiftsbiträden får därför förutsättas ha ordnat sin behandling så att exempelvis en begäran om information från en registrerad som inkommit men inte hunnit besvaras före den 25 maj 2018 kan tillmötesgås i enlighet med förordningens bestämmelser. Även tillsynsmyndighetens verksamhet bör i möjligaste mån ha anpassats till förordningens regelverk vid denna tidpunkt.

Tillsynsärenden kan dock pågå under en längre tid och det är inte självklart att tillsynsmyndigheten helt kan styra över när underlaget är så fullständigt att beslut i ärendet kan fattas. Utredningen föreslår mot denna bakgrund en övergångsbestämmelse om att ärenden som har inletts hos Datainspektionen före ikraftträdandet av dataskyddslagen men som vid den tidpunkten ännu inte har avgjorts, ska handläggas enligt personuppgiftslagen.

Datainspektionen invänder dock mot detta förslag och anför att behandling av personuppgifter i de allra flesta fall är en pågående aktivitet samt att pågående behandling ska bedömas enligt regleringen i dataskyddsförordningen från och med den 25 maj 2018. Regeringen bedömer mot denna bakgrund att det inte finns skäl att införa någon sådan övergångsbestämmelse som utredningen föreslår. Det bör dock noteras att personuppgiftslagen i vissa fall ändå kommer att vara tillämplig även hos Datainspektionen, nämligen vid tillsyn över behandling av personuppgifter som fortfarande regleras av personuppgiftslagen eller författningar som hänvisar till personuppgiftslagen, se föregående avsnitt.

Utredningen föreslår vidare en övergångsbestämmelse om att äldre föreskrifter fortfarande gäller för överklagande av beslut som har meddelats med stöd av personuppgiftslagen. Regeringen anser i likhet med utredningen att en sådan övergångsbestämmelse behövs, vilket inte heller ifrågasätts av remissinstanserna. Som *Förvaltningsrätten i Malmö* påpekar bör dock uttrycket äldre föreskrifter inte användas, eftersom detta skulle kunna tolkas som att det tar sikte på föreskrifter i andra författningar än den som upphävs genom dataskyddslagen. I stället bör det av övergångsbestämmelsen framgå att den upphävda lagen, dvs. personuppgiftslagen, fortfarande gäller för överklagande av beslut som har meddelats med stöd av den lagen. Motsvarande övergångsbestämmelse bör införas avseende anslutande författningar till personuppgiftslagen, dvs. personuppgiftsförordningen och Datainspektionens föreskrifter.

Skadestånd

I 48 § PUL finns bestämmelser om skadeståndsskyldighet för personuppgiftsansvariga och möjlighet att jämka sådan skadeståndsskyldighet i vissa fall. Genom dataskyddsförordningen utvidgas skadeståndsansvaret till att gälla även personuppgiftsbiträden. Vidare gäller rätten till

skadestånd enligt dataskyddsförordningen även vid skada som uppstått på grund av överträdelser av dataskyddslagen och andra föreskrifter som kompletterar dataskyddsförordningen.

Utredningen föreslår en övergångsbestämmelse som anger att äldre föreskrifter om skadestånd fortfarande ska gälla för skada som har orsakats före ikraftträdandet. Det följer emellertid redan av allmänna grundsatser att ny lagstiftning ska gälla i fråga om skadestånd med anledning av skadefall som inträffar efter ikraftträdandet, medan äldre lag ska tillämpas på skadefall som har inträffat dessförinnan (prop. 1972:5 s. 593). Någon särskild övergångsbestämmelse om detta behövs inte. Utredningens förslag i denna del bör därför inte genomföras.

Straffbestämmelsens avskaffande

Eftersom förslaget innebär att den straffrättsliga regleringen upphävs och i praktiken ersätts med sanktionsavgifter, uppkommer frågan om vad som ska gälla för straffbelagda gärningar som har begåtts vid behandling som har upphört före den 25 maj 2018 men där överträdelsen inte har lagförts innan de nya reglerna ska börja tillämpas.

Vid bedömningen av behovet att meddela övergångsbestämmelser för den nu nämnda situationen behöver bestämmelserna i såväl 2 kap. 10 § RF som 5 § andra stycket lagen (1964:163) om införande av brottsbalken beaktas.

I 2 kap. 10 § RF finns ett förbud mot retroaktiv straff- och skattelagstiftning. Förbudet mot retroaktiv skattelag anses analogivis tillämpligt beträffande straffliknande administrativa påföljder. Att ta ut sanktionsavgifter för överträdelser som begåtts före den 25 maj 2018 skulle således kunna strida mot retroaktivitetsförbudet.

Av 5 § andra stycket lagen om införande av brottsbalken framgår att straff ska bestämmas enligt den lag som gällde när gärningen företogs. Detta är dock inte fallet om annan lag gäller när dom meddelas, under förutsättning att den nya lagen leder till frihet från straff eller till lindrigare straff. Denna bestämmelse har enligt förarbetena generell räckvidd, dvs. den gäller även utanför brottsbalkens tillämpningsområde (prop. 1964:10 s. 99). Bestämmelsen ger uttryck för den lindrigaste lagens princip.

Bestämmelserna i dataskyddsförordningen och dataskyddslagen innebär att överträdelser av den gällande dataskyddsregleringen överförs från det straffrättsliga området till ett system med enbart sanktionsavgifter. Formellt sett får sanktionsavgiften anses lindrigare och borde därmed få genomslag bakåt i tiden. Huvudsyftet med dataskyddsförordningens och dataskyddslagens system med kraftfulla sanktionsavgifter är emellertid framför allt att effektivisera sanktionssystemet. Att överträdelser mot dataskyddsregleringen föreslås avkriminaliseras ska inte ses som ett uttryck för att överträdelserna ska bedömas lindrigare än tidigare. Regeringen anser därför, i likhet med utredningen och till skillnad från *Datainspektionen*, att lindrigaste lagens princip inte gör sig särskilt starkt gällande i detta fall. Det finns därför inte skäl att låta systemet med sanktionsavgifter få retroaktiv effekt. För ett liknande resonemang rörande sanktionsväxling, se prop. 2007/08:107 och prop. 2012/13:143 s. 82.Personuppgiftslagens straffbestämmelse bör i

stället tillämpas på överträdelser som skett före dataskyddslagens ikraftträdande.

Beslut om behandling av personuppgifter som rör lagöverträdelser

Av 21 § fjärde stycket PUL och 9 § PUF följer att Datainspektionen får meddela beslut i enskilda fall om undantag från förbudet för andra än myndigheter att behandla personuppgifter om lagöverträdelser som innefattar brott, domar i brottmål, straffprocessuella tvångsmedel eller administrativa frihetsberövanden. I avsnitt 11 föreslår regeringen att den myndighet som regeringen bestämmer på motsvarande sätt ska ges befogenhet att i enskilda fall besluta att andra än myndigheter får behandla sådana uppgifter som avses i artikel 10 i dataskyddsförordningen, dvs. personuppgifter som rör lagöverträdelser. *Svensk Försäkring* anser att en övergångsbestämmelse bör övervägas som klargör att nu gällande tillstånd att behandla sådana personuppgifter gäller även fortsättningsvis. Regeringen är av samma uppfattning. Det bör således av tydlighetsskäl införas en övergångsbestämmelse till dataskyddslagen som anger att beslut i enskilda fall avseende behandling av personuppgifter som rör lagöverträdelser och som har meddelats med stöd av personuppgiftslagen fortfarande ska gälla.

19 Konsekvenser

19.1 Ekonomiska konsekvenser för det allmänna

Regeringens bedömning: Förslagen innebär att tillsynsmyndigheten och de allmänna förvaltningsdomstolarna får något fler arbetsuppgifter, men kostnadsökningarna kommer inte att bli större än att de ryms inom de befintliga anslagen.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Det stora flertalet remissinstanser instämmer i utredningens bedömning eller kommenterar den inte. *Södertörns tingsrätt* anser att det är svårt att närmare se vilka konsekvenser förslaget kommer att få för domstolarna innan det står klart hur domstolarnas registerförfattningar kommer att anpassas. *Kammarrätten i Stockholm* påpekar att förslagen troligtvis kommer att medföra en ökad måltillströmning. *Förvaltningsrätten i Linköping* anser att arbetsuppgifterna kommer att öka för förvaltningsrätterna, även om måltillströmningens omfattning i nuläget kan vara svår att uppskatta. Förvaltningsrätten anser att genomförandet av förslaget kommer att bli mer resurskrävande än vad genomförandet av ny lagstiftning normalt sett är och att det därför framstår som mycket tveksamt om genomförandet ryms inom de berörda myndigheternas anslag. *Domstolsverket* vill framhålla det problematiska i att det inte i något sammanhang görs en samlad bedömning av de konsekvenser som reformen i sin helhet medför. *Pensionsmyndigheten* instämmer i utredningens bedömning att dataskyddsförordningens direkt tillämpliga bestämmelser och tillhörande nationella regler kan förväntas

öka kostnaderna för personuppgiftsansvariga myndigheter. Pensionsmyndigheten anser att det är rimligt, eftersom förordningen leder till ökad rättssäkerhet och förutsebarhet för enskilda. De ökade kostnaderna måste dock enligt Pensionsmyndigheten beaktas när riksdagen och regeringen beslutar om budget och medel för myndigheterna, eftersom annan verksamhet annars konkurreras ut. *Kronofogdemyndigheten* anser att förslaget om verkställighet av sanktionsavgifter sannolikt medför en viss ökning av Kronofogdens utsökningsärenden och kan därför medföra kostnadsökningar för myndigheten. *Centrala studiestödsnämnden* anför att nämnden inte kommer att ha några direkta kostnader kopplade till utredningens förslag, vid sidan av den risk som gäller generellt för myndigheterna att påföras sanktionsavgift. Däremot menar nämnden att översynen och anpassningen av verksamhetens system och organisation efter dataskyddsförordningens krav kommer att medföra kostnader för myndigheten. *Konkurrensverket* bedömer att de nya reglerna kan komma att ha stora och svårförutsägbara konsekvenser för svensk offentlig förvaltning. Konkurrensverket anser att det hade varit värdefullt om reglernas innebörd och konsekvenser för svenska myndigheter hade utretts redan under arbetet med den nya regleringen. *Malmö kommun* och *Piteå kommun* anser att dataskyddsförordningen och de kompletterande nationella bestämmelserna kan medföra ökade kostnader, men att flesta kostnaderna är relaterade till genomförandet av dataskyddsförordningen. De anser dock att det finns viss risk för ökade kostnader när det gäller möjligheten att ta ut höga sanktionsavgifter av myndigheter. *Stockholms kommun* instämmer i bedömningen att det är dataskyddsförordningen och inte det aktuella lagförslaget som kommer att medföra ökad administration och kostnader för kommunen. *Skurups kommun* anser att det är en brist att utredningen inte har haft i uppdrag att utreda vilka konsekvenser dataskyddsförordningen kommer att innebära för det allmänna.

Skälen för regeringens bedömning: Som flera av remissinstanser påpekar, bl.a. *Centrala studiestödsnämnden*, *Konkurrensverket* och *Stockholms kommun*, står det klart att dataskyddsförordningens direkt tillämpliga bestämmelser kommer att leda till vissa konsekvenser för det allmänna. Förordningens bestämmelser kan bl.a. komma att öka kostnaderna för myndigheter i form av ökad administration och ökade kostnader initialt för anpassning av befintliga it-system. Det kommer också att krävas ökade resurser till utbildningsinsatser och eventuellt nyrekryteringar till tjänster som dataskyddsombud. Konsekvenserna av dataskyddsförordningens direkt tillämpliga bestämmelser behandlas dock inte i detta lagstiftningsärende.

Domstolsverket anser att det är problematiskt att det inte i något sammanhang görs en samlad bedömning av de konsekvenser som reformen i sin helhet medför. Liknande synpunkter lämnas av bl.a. *Skurups kommun*. Regeringen kan dock konstatera att någon sådan samlad konsekvensanalys inte går att utföra i ett enskilt lagstiftningsärende. Flertalet nationella bestämmelser som kompletterar dataskyddsförordningen kommer att finnas i de sektorsspecifika författningarna om behandling av personuppgifter och det är först när samtliga förslag till anpassningar av dessa författningar har lagts fram som det skulle vara möjligt att göra en samlad bedömning. Värdet av en sådan bedömning skulle dessutom kunna ifrågasättas, eftersom det bara kommer att vara

dataskyddslagen som, vid sidan av dataskyddsförordningen, gäller för samtliga myndigheter.

Utredningen bedömer att förslagen medför nya arbetsuppgifter för tillsynsmyndigheten och de allmänna förvaltningsdomstolarna. Flera av dessa nya arbetsuppgifter är emellertid kopplade till utredningens förslag om åtgärder vid tillsynsmyndighetens dröjsmål. Eftersom regeringen inte föreslår att dessa förslag ska genomföras uppstår inga nya arbetsuppgifter för tillsynsmyndigheten och domstolarna i den delen.

Däremot föreslår regeringen, i enlighet med utredningens förslag, att det genom lagen ska införas en möjlighet för tillsynsmyndigheten att påföra en myndighet sanktionsavgifter. I likhet med utredningen anser dock regeringen att sådana beslut får antas bli sällsynta. Det beror dels på att myndigheter i regel kan förväntas anpassa verksamheten efter tillsynsmyndighetens synpunkter utan att det krävs repressiva åtgärder, dels på att sanktionsavgift är den åtgärd som tillsynsmyndigheten bör välja som sista alternativ. Det bör därför inte påverka tillsynsmyndighetens arbetsbörda i någon större utsträckning.

Förslaget innebär även att sanktionsavgifter ska kunna påföras vid överträdelser av artikel 10 i dataskyddsförordningen, dvs. vid behandling av personuppgifter som rör lagöverträdelser. För tillsynsmyndighetens del utgör detta en ny arbetsuppgift i förhållande till vad som följer av dataskyddsförordningen. Regeringen vill dock betona att tillsynsmyndigheten också enligt personuppgiftslagen har möjlighet att vidta åtgärder mot den personuppgiftsansvarige vid behandling av personuppgifter som rör lagöverträdelser. Det bör särskilt noteras att tillsynsmyndigheten enligt personuppgiftslagen har möjlighet att förena förelägganden med vite, en möjlighet som nu försvinner och ersätts med systemet med sanktionsavgifter. Sammanfattningsvis anser regeringen att kostnaderna för tillsynsmyndigheten bör rymmas inom befintliga anslagsramar såvitt avser förslagen i detta lagstiftningsärende. I det sammanhanget kan nämnas att Datainspektionens anslag har ökats med anledning av dataskyddsförordningen (prop. 2017/18:1 utgiftsområde 1, del 9).

Eftersom sanktionsavgifterna kan vara ekonomiskt kännbara är det rimligt att utgå från att inspektionens beslut kommer att överklagas till allmän förvaltningsdomstol i relativt stor utsträckning. Det faktum att sådana beslut mot myndigheter förväntas bli ovanliga innebär dock att även överklagandena bör bli sällsynta. Det är svårt att uppskatta hur vanligt det kommer att bli att tillsynsmyndigheten beslutar om sanktionsavgifter vid överträdelser av artikel 10, men sannolikt kommer det inte bli fråga om särskilt många beslut per år. Däremot kan det antas att dessa mer eller mindre regelmässigt kommer att överklagas till allmän förvaltningsdomstol.

Som nämns ovan har tillsynsmyndigheten enligt personuppgiftslagen möjlighet att förena förelägganden med vite. Vid utdömande av sådana viten krävs domstolsprövning enligt viteslagen. Eftersom möjligheten att vitesförelägga försvinner enligt regeringens förslag, kommer mål om utdömande av sådana viten inte längre att förekomma i allmän förvaltningsdomstol. Med tanke på att tillsynsmyndigheten inte har utnyttjat sin möjlighet att vitesförelägga enligt personuppgiftslagen och det ännu är oklart i vilken mån sanktionsavgifter kommer att tillgripas i motsvarande

situationer, kan det dock inte uteslutas att domstolarnas arbetsbelastning ändå kan komma att öka något. Kostnaderna för de allmänna förvaltningsdomstolarna bör emellertid rymmas inom befintliga anslagsramar såvitt avser förslagen i detta lagstiftningsärende.

19.2 Ekonomiska konsekvenser för enskilda

Regeringens bedömning: Förslagen medför inga nya kostnader eller någon ökad administrativ börda för enskilda.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Det stora flertalet remissinstanser instämmer i utredningens bedömning eller kommenterar den inte. *Tillväxtverket* ser inte att det finns något som talar emot utredningens bedömning. *Företagarna* anser att införandet av dataskyddsförordningen kommer att få stora konsekvenser för företag, men att de förslag som utredningen föreslår är en försumbar del av dessa konsekvenser. Företagarna anser att det är viktigt att tillämpningen följs upp så att inte mindre företag slås ut från branscher där det är en omfattande behandling av personuppgifter på grund av kraven på konsekvensbedömningar m.m. Företagarna påpekar vidare att många ideella föreningar kommer att drabbas av ökade krav vad gäller hanteringen av personuppgifter. *Småföretagarnas Riksförbund* anser att utredningen inte har följt kommittédirektiven beträffande konsekvensbeskrivningar där utredaren särskilt ska ange konsekvenserna för företagen i form av kostnader och administrativa bördor. Vidare menar förbundet att utredningen inte tydligt har redovisat hur förslagen utformats så att företagens administrativa börda inte ökar mer än nödvändigt. Införandet av en ny dataskyddslag är sammankopplat med dataskyddsförordningen och det finns enligt förbundet en stor oro bland landets små företag beträffande denna. För att små företag ska kunna säkerställa att göra rätt uppstår det kostnader för utbildning av personal, utbildning för personuppgiftsbiträde samt översyn och nya rutiner beträffande registerhantering, vilket enligt förbundet borde ha behandlats i konsekvensavsnittet. Några instanser, bl.a. *Svenskt friluftsliv*, *Svenska Brukshundklubben* och *Villaägarnas riksförbund*, anser att det är anmärkningsvärt att lagförslagens inverkan på föreningar och civilsamhället inte nämns av utredningen. *Näringslivets regelnämnd* anser att utredningens slutsats att förslagen inte medför några kostnader eller någon ökad administrativ börda för företagen är felaktig och att betänkandets konsekvensanalys behöver kompletteras. Nämnden menar bl.a. att negativa konsekvenser för företag som en följd av den befintliga sekretessregleringen hos tillsynsmyndigheten behöver utredas och att alternativet med absolut sekretess behöver övervägas och konsekvensutredas.

Skälen för regeringens bedömning: Som flera av remissinstanser påpekar, bl.a. *Företagarna*, *Småföretagarnas riksförbund*, *Svenskt friluftsliv* och *Näringslivets regelnämnd*, står det klart att dataskyddsförordningens direkt tillämpliga bestämmelser kommer att leda till vissa konsekvenser för företag, ideella föreningar och andra enskilda organ. Förordningens bestämmelser kan i vissa fall förväntas leda till ökade

kostnader för administration och för anpassning av befintliga it-system. Det kommer också att krävas ökade resurser till utbildningsinsatser och eventuellt nyrekryteringar till tjänster som dataskyddsombud. Å andra sidan bedömde EU-kommissionen, i sin konsekvensbedömning av förslaget till dataskyddsförordning, att reformen kommer att stärka den inre marknaden och enbart vad gäller administrativa bördor göra det möjligt för företagen att sammanlagt spara ca 2,3 miljarder euro per år (SEK[2012] 73 final). Oaktat hur det förhåller sig med detta kan regeringen konstatera att konsekvenserna av dataskyddsförordningens direkt tillämpliga bestämmelser inte påverkar behovet, lämpligheten och konsekvenserna av de förslag som lämnas i detta lagstiftningsärende. Dessa konsekvenser redovisas därför inte här.

Av relevans för analysen är vidare endast sådana förslag som medför förändringar för företag och andra enskilda organ, i relation till vad som gäller i dag. De förslag som lämnas i detta lagstiftningsärende medför inga sådana förändringar. Om dataskyddsförordningens direkt tillämpliga bestämmelser leder till en ökad benägenhet att efterleva regelverket som helhet är det givetvis positivt. De eventuella kostnadsökningar som detta medför kan dock inte beaktas, eftersom utgångspunkten måste vara att samtliga aktörer redan följer gällande rätt. Mot denna bakgrund kan regeringen, i likhet med *Tillväxtverket*, inte se att förslagen i detta lagstiftningsärende leder till några kostnadsökningar eller någon ökad administrativ börda för enskilda.

19.3 Konsekvenser i övrigt

Regeringens bedömning: Förslagen förväntas förbättra skyddet för enskildas personliga integritet. De förväntas inte få några andra konsekvenser.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna kommenterar inte utredningens bedömning i denna del.

Skälen för regeringens bedömning: Förslagen innebär bl.a. att det införs särskilda bestämmelser om myndigheternas behandling av känsliga personuppgifter. Avsikten med förslagen i denna del är inte att utvidga möjligheterna till behandling i relation till vad som gäller i dag, utan att i stort sett möjliggöra behandling i motsvarande utsträckning som enligt personuppgiftslagen och personuppgiftsförordningen. Det föreslås dock också ett förbud för myndigheter som behandlar uppgifter med stöd av dessa bestämmelser att utföra sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter. Sökbegränsningen saknar motsvarighet i dag. Regeringen bedömer att det förslaget gynnar enskildas personliga integritet.

Dataskyddsförordningens bestämmelser innebär en förstärkning av enskildas rätt till information och tillgång till personuppgifter jämfört med motsvarande reglering i personuppgiftslagen. De undantag regeringen föreslår från förordningens bestämmelser i detta avseende motsvarar de befintliga undantagen i personuppgiftslagen, trots att mer långtgående undantag i och för sig hade varit möjliga. Regeringen

bedömer därför att regleringen sammantaget innebär en förstärkning av skyddet för enskildas personliga integritet.

Vidare bör den föreslagna möjligheten att besluta om sanktionsavgifter mot myndigheter när det gäller felaktig behandling av enskildas personuppgifter öka skyddet för enskildas personliga integritet. Den föreslagna tystnadsplikten för dataskyddsombud innebär slutligen också ett stärkt skydd för den personliga integriteten.

Förslagen kommer att gälla även för personuppgiftsbehandling som sker hos kommuner och landsting, men får inte några särskilda konsekvenser för dessa organ eller för den kommunala självstyrelsen.

Författningsförslagen är könsneutralt utformade och förväntas inte få några konsekvenser för jämställdheten mellan kvinnor och män.

20 Författningskommentar

20.1 Förslaget till lag med kompletterande bestämmelser till EU:s dataskyddsförordning

1 kap. Inledande bestämmelser

1 § Denna lag kompletterar Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), här benämnd EU:s dataskyddsförordning.

Termer och uttryck i denna lag har samma betydelse som i EU:s dataskyddsförordning. Med känsliga personuppgifter avses i denna lag sådana uppgifter som avses i artikel 9.1 i EU:s dataskyddsförordning.

Paragrafen anger lagens innehåll. Övervägandena finns i avsnitt 5.1.

I *första stycket* anges att lagen innehåller kompletterande bestämmelser till dataskyddsförordningen. Detta innebär att lagen inte kan tillämpas fristående, utan endast tillsammans med dataskyddsförordningen. Lagen innehåller de kompletterande bestämmelser som gäller på ett generellt plan. Det finns även sektorsspecifika författningar som innehåller bestämmelser som kompletterar dataskyddsförordningen för vissa myndigheter eller inom vissa områden. Som exempel kan nämnas patientdatalagen, studiestödsdatalagen och utlänningsdatalagen. Hänvisningarna i lagen till dataskyddsförordningen är med undantag för 2 § och 6 kap. 3 och 4 §§ dynamiska, dvs. avser förordningen i den vid varje tidpunkt gällande lydelsen.

Av *andra stycket* framgår att de termer och uttryck som används i lagen ska förstås på samma sätt som i dataskyddsförordningen. Det innebär bl.a. att definitionerna i artikel 4 i dataskyddsförordningen även gäller vid tillämpningen av lagen. Vidare framgår att med känsliga personuppgifter avses i lagen sådana uppgifter som tillhör de särskilda kategorier av personuppgifter som anges i artikel 9.1 i dataskyddsförordningen. De särskilda kategorier av personuppgifter som anges i den artikeln är personuppgifter som avslöjar ras eller etniskt ursprung,

politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening samt genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa och uppgifter om en fysisk persons sexualliv eller sexuella läggning.

Tillämpningsområde

2 § EU:s dataskyddsförordning, i den ursprungliga lydelsen, ska i tillämpliga delar gälla även vid behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av unionsrätten och i verksamhet som omfattas av avdelning V kapitel 2 i fördraget om Europeiska unionen. Denna lag kompletterar EU:s dataskyddsförordning även vid sådan behandling.

Genom paragrafen, som saknar motsvarighet i personuppgiftslagen, utsträcks det materiella tillämpningsområdet för dataskyddsförordningens bestämmelser. Övervägandena finns i avsnitt 6.1.1.

Av paragrafen framgår att dataskyddsförordningen i tillämpliga delar ska gälla även vid personuppgiftsbehandling som utförs som ett led i en verksamhet som inte omfattas av unionsrätten och i verksamhet som utförs inom ramen för den gemensamma utrikes- och säkerhetspolitiken. Det framgår också att lagen kompletterar dataskyddsförordningen även vid sådan behandling. Förordningens bestämmelser, i tillämpliga delar, gäller alltså som svensk rätt även vid personuppgiftsbehandling som utförs i sådan verksamhet som enligt artikel 2.2 a och 2.2 b i dataskyddsförordningen är undantagen från förordningens tillämpningsområde. Att förordningen gäller i tillämpliga delar innebär att de flesta av förordningens bestämmelser gäller, t.ex. bestämmelserna om principer för behandling av personuppgifter, de registrerades rättigheter och de personuppgiftsansvarigas skyldigheter. Verksamhet som inte omfattas av unionsrättens tillämpningsområde är bl.a. verksamhet som rör nationell säkerhet. Som exempel kan nämnas verksamhet på försvarsområdet.

Genom att det i paragrafen anges att dataskyddsförordningen ska gälla inom de angivna verksamheterna i tillämpliga delar tydliggörs att sådana bestämmelser i förordningen som inte kan tillämpas i rent nationella sammanhang inte gäller. Som exempel kan nämnas bestämmelserna som rör uppförandekoder och certifiering, till den del de avser kommissionens och Europeiska dataskyddsstyrelsens roll (t.ex. artiklarna 40.11 och 42.8). De bestämmelser som ger kommissionen befogenheter i fråga om överföring till tredjeland (artikel 45) är inte tillämpliga och inte heller bestämmelserna som ålägger kommissionen skyldigheter i fråga om uppföljande åtgärder (artiklarna 97 och 98). Vidare är det inte möjligt att genom nationell rätt ålägga tillsynsmyndigheter i andra länder att samarbeta med den svenska tillsynsmyndigheten. Det är inte heller möjligt att ge Europeiska dataskyddsstyrelsen behörighet att t.ex. utfärda riktlinjer och rekommendationer eller att ge kommissionen rätt att anta delegerade akter inom detta område. Kapitel VII och kapitel X i dataskyddsförordningen är därför inte tillämpliga. Hänvisningen till dataskyddsförordningen är statisk, dvs. avser den ursprungliga lydelsen av förordningen.

3 § Bestämmelserna i 2 § gäller inte i verksamhet som omfattas av

1. lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst,
2. lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet, eller
3. 6 kap. polisdatalagen (2010:361).

Paragrafen, som saknar motsvarighet i personuppgiftslagen, reglerar undantag från den bestämmelse i lagen som utsträcker dataskyddsförordningens tillämpningsområde. Övervägandena finns i avsnitt 6.1.1.

I paragrafen anges att 2 § inte gäller i verksamhet som omfattas av lagen om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst, lagen om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet eller 6 kap. polisdatalagen. Detta innebär att dataskyddsförordningens och lagens bestämmelser inte gäller i sådan verksamhet.

Även i sektorsspecifika författningar som avser verksamhet utanför dataskyddsförordningens egentliga tillämpningsområde kan det föreskrivas undantag från bestämmelsen i 2 §, se 6 §. Det kan i sådana författningar också anges att endast vissa av dataskyddsförordningens bestämmelser inte ska gälla inom just det området.

4 § Artiklarna 33 och 34 i EU:s dataskyddsförordning tillämpas inte i fråga om personuppgiftsincidenter som ska rapporteras enligt säkerhetsskyddslagen (1996:627) eller föreskrifter som har meddelats i anslutning till den lagen.

Paragrafen, som saknar motsvarighet i personuppgiftslagen, reglerar undantag från den bestämmelse i lagen som utsträcker dataskyddsförordningens tillämpningsområde, när det gäller vissa personuppgiftsincidenter. Övervägandena finns i avsnitt 6.1.2.

Enligt paragrafen ska dataskyddsförordningens bestämmelser i artiklarna 33 och 34 om personuppgiftsincidenter inte tillämpas i fråga om incidenter som ska rapporteras enligt säkerhetsskyddslagen eller föreskrifter som har meddelats i anslutning till den lagen. Detta innebär att sådana incidenter som enligt 10 a § första stycket säkerhetsskyddsförordningen ska anmälas till den myndighet som utövar tillsyn över säkerhetsskyddet, dvs. Försvarsmakten eller Säkerhetspolisen, inte också ska rapporteras till tillsynsmyndigheten enligt dataskyddsförordningen. Vid en sådan incident gäller inte heller skyldigheten enligt dataskyddsförordningen att informera de registrerade.

5 § Denna lag gäller vid behandling av personuppgifter som utförs av personuppgiftsansvariga eller personuppgiftsbiträden som är etablerade i Sverige, om behandlingen utförs inom ramen för verksamhet som bedrivs vid verksamhetsställen här i landet. Lagen gäller även vid behandling av personuppgifter som utförs av personuppgiftsansvariga som är etablerade på en annan plats där svensk rätt gäller enligt folkrätten.

Lagen gäller också vid behandling av personuppgifter som utförs av personuppgiftsansvariga eller personuppgiftsbiträden som endast är etablerade i tredjeland, om behandlingen avser registrerade som befinner sig i Sverige och har anknytning till
1. utbjudande av varor eller tjänster till sådana registrerade, eller
2. övervakning av deras beteende i Sverige.

Bestämmelsen i 2 kap. 1 § gäller vid behandling av personuppgifter som avser barn som bor i Sverige, oavsett var de personuppgiftsansvariga eller personuppgiftsbiträdena är etablerade.

I paragrafen, som delvis motsvarar 4 § PUL, finns bestämmelser om lagens territoriella tillämpningsområde. Övervägandena finns i avsnitt 6.2.

Huvudregeln i *första stycket första meningen* anger att lagen gäller vid behandling av personuppgifter som utförs av personuppgiftsansvariga eller personuppgiftsbiträden som är etablerade i Sverige. För att lagen ska vara tillämplig krävs därutöver att den aktuella behandlingen av personuppgifter utförs inom ramen för den verksamhet som bedrivs vid det svenska verksamhetsstället. Det saknar betydelse var den faktiska behandlingen sker. Lagen är däremot, enligt huvudregeln, inte tillämplig vid behandling av personuppgifter som sker endast inom ramen för verksamhet vid ett verksamhetsställe i ett annat land, även om behandlingen avser uppgifter om personer i Sverige och även om den personuppgiftsansvarige också har ett verksamhetsställe i Sverige. Med begreppet verksamhetsställe avses detsamma som i dataskyddsförordningen (jfr skäl 22). Personuppgiftsansvariga och personuppgiftsbiträden bör således anses etablerade genom ett verksamhetsställe i Sverige om de bedriver en faktisk och reell verksamhet med hjälp av en stabil struktur här i landet. Det kan t.ex. vara fråga om ett dotterbolag eller en filial, men den rättsliga formen för en sådan struktur bör inte vara en avgörande faktor. Enligt *första stycket andra meningen* gäller lagen också för personuppgiftsansvariga som är etablerade på en annan plats där svensk rätt gäller enligt folkrätten. Med detta begrepp avses detsamma som i dataskyddsförordningen (jfr skäl 25). Det innebär exempelvis att behandling av personuppgifter som sker vid svenska utlandsmyndigheter omfattas av lagens bestämmelser.

Genom *andra stycket* klargörs att lagen under vissa förutsättningar också gäller för personuppgiftsansvariga och personuppgiftsbiträden som endast är etablerade i tredjeland, dvs. som saknar verksamhetsställe inom EU, i den mån dessa behandlar personuppgifter om registrerade som befinner sig i Sverige. För att lagen ska vara tillämplig krävs att behandlingen rör antingen utbjudande av varor eller tjänster till sådana registrerade eller övervakning av deras beteende i Sverige. Med övervakning av registrerades beteende avses detsamma som i dataskyddsförordningen. Av skäl 24 till förordningen framgår att det, för att avgöra om en viss behandling kan anses övervaka beteendet hos de registrerade, bör fastställas om fysiska personer spåras på internet, i synnerhet om syftet är att fatta beslut rörande dessa personer eller att analysera eller förutsäga deras personliga preferenser, beteende och attityder.

Genom *tredje stycket* görs undantag från etableringslandsprincipen i fråga om bestämmelsen om barns samtycke i 2 kap. 1 §. Den åldersgräns som anges där gäller vid behandling av personuppgifter som avser barn som bor i Sverige, oavsett var de personuppgiftsansvariga eller personuppgiftsbiträdena är etablerade (se författningskommentaren till 2 kap. 1 §).

Avvikande bestämmelser i annan författning

6 § Om en annan lag eller en förordning innehåller någon bestämmelse som avviker från denna lag, tillämpas den bestämmelsen.

Paragrafen reglerar lagens förhållande till avvikande bestämmelser i andra författningar. Paragrafen motsvarar 2 § PUL. Övervägandena finns i avsnitt 5.1.3.

I paragrafen anges att om en annan lag eller en förordning innehåller någon bestämmelse som avviker från lagen tillämpas den bestämmelsen. Avvikande bestämmelser som finns i en annan lag eller i en förordning ska alltså ha företräde framför lagen. Det kan t.ex. vara bestämmelser som specificerar eller begränsar rätten att behandla känsliga personuppgifter i en viss verksamhet eller särskilda förfaranderegler. Sådana avvikande bestämmelser som avses i paragrafen finns ofta i författningar som helt eller delvis innehåller bestämmelser om behandling av personuppgifter hos en viss myndighet, inom en viss sektor eller i ett visst sammanhang. Författningar av detta slag förekommer främst för den offentliga sektorn. Som exempel kan nämnas patientdatalagen, studiestödsdatalagen och utlänningsdatalagen. Begreppet en annan lag omfattar inte bara avvikande bestämmelser i lagar antagna av riksdagen, utan även bestämmelser i direkt tillämpliga EU-förordningar.

Begränsningen i bestämmelsen till avvikande bestämmelser i lag och förordning innebär att myndighetsföreskrifter inte har företräde framför lagen.

Bestämmelsen innebär endast en möjlighet att avvika från lagen och inte en möjlighet att införa bestämmelser som avviker från dataskyddsförordningen.

Förhållandet till tryck- och yttrandefriheten

7 § EU:s dataskyddsförordning och denna lag ska inte tillämpas i den utsträckning det skulle strida mot tryckfrihetsförordningen eller yttrandefrihetsgrundlagen.

Artiklarna 5–30 och 35–50 i EU:s dataskyddsförordning samt 2–5 kap. denna lag ska inte tillämpas på behandling av personuppgifter som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande.

Paragrafen, som reglerar dataskyddsförordningens och lagens förhållande till tryckfrihetsförordningen och yttrandefrihetsgrundlagen, motsvarar 7 § och 8 § första stycket PUL. Övervägandena finns i avsnitt 7.

I paragrafens *första stycke* anges att dataskyddsförordningen och lagen inte ska tillämpas i den utsträckning det skulle strida mot tryckfrihetsförordningen eller yttrandefrihetsgrundlagen. Bestämmelsen tydliggör att tryckfrihetsförordningen och yttrandefrihetsgrundlagen har företräde framför dataskyddsförordningens och lagens bestämmelser.

I *andra stycket*, som har sin grund i artikel 85.2 i dataskyddsförordningen, anges att artiklarna 5–30 och 35–50 i dataskyddsförordningen och 2–5 kap. i lagen inte ska tillämpas på behandling av personuppgifter för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande utanför det grundlagsreglerade området. Bestämmelsen innebär att endast bestämmelserna om syfte, tillämpningsområde

och definitioner (kapitel I), om samarbete med tillsynsmyndigheten och säkerhet för personuppgifter (artiklarna 31–34 i kapitel IV), om oberoende tillsynsmyndigheter (kapitel VI), om samarbete och enhetlighet (kapitel VII) samt om rättsmedel, ansvar och sanktioner (kapitel VIII) är tillämpliga på behandling för de nämnda ändamålen. Bestämmelserna om tillsyn, rättsmedel, ansvar och sanktioner är därmed i praktiken tillämpliga enbart såvitt avser tillsyn över eller överträdelser av bestämmelserna om säkerhet för personuppgifter.

Tystnadsplikt för dataskyddsombud

8 § Den som fullgör uppgift som dataskyddsombud enligt artikel 37 i EU:s dataskyddsförordning får inte obehörigen röja det som han eller hon vid fullgörandet av sin uppgift har fått kännedom om.

I det allmännas verksamhet tillämpas offentlighets- och sekretesslagen (2009:400) i stället för första stycket.

Paragrafen, som saknar motsvarighet i personuppgiftslagen, reglerar tystnadsplikt för dataskyddsombud. Övervägandena finns i avsnitt 15.2.

Paragrafen har sin grund i artikel 38.5 i dataskyddsförordningen.

Enligt *första stycket* gäller tystnadsplikt för det som den som fullgör uppgift som dataskyddsombud får kännedom om vid fullgörandet av sin uppgift. Tystnadsplikten är dock begränsad till obehörigt röjande av uppgifter. Det innebär att uppgifter får lämnas ut till exempelvis tillsynsmyndigheten eller annars som en följd av en skyldighet i lag eller annan författning, eftersom ett sådant röjande inte kan anses vara obehörigt.

Andra stycket innehåller en erinran om att offentlighets- och sekretesslagen tillämpas i det allmännas verksamhet. Om ett dataskyddsombud innehar en sådan anställning eller ett sådant uppdrag som avses i 2 kap. 1 § andra stycket OSL och deltar i myndighetens verksamhet, omfattas han eller hon av den sekretess som gäller hos myndigheten. Ett dataskyddsombud som har utnämnts av en myndighet får i allmänhet anses delta i myndighetens verksamhet på ett sådant sätt som förutsätts i den bestämmelsen.

2 kap. Rättslig grund för behandling av personuppgifter

Barns samtycke

1 § Vid erbjudande av informationssamhällets tjänster direkt till ett barn som bor i Sverige ska behandling av personuppgifter vara tillåten med stöd av barnets samtycke, om barnet är minst 13 år. Om barnet är under 13 år, ska sådan behandling vara tillåten endast om samtycke ges eller godkänns av den person som har föräldraansvar för barnet.

Paragrafen reglerar vid vilken ålder barn som erbjuds informationssamhällets tjänster själva kan samtycka till behandling av personuppgifter. Paragrafen har ingen motsvarighet i personuppgiftslagen. Övervägandena finns i avsnitt 9.

Bestämmelsen har sin grund i artikel 8.1 i dataskyddsförordningen, som anger att sådan behandling av personuppgifter som avses i paragrafen får ske med stöd av barnets eget samtycke, om barnet har fyllt

16 år. Medlemsstaterna får föreskriva en lägre åldersgräns, dock lägst 13 år.

Genom bestämmelsen bestäms åldersgränsen i Sverige till 13 år. Bestämmelsen gäller för barn som bor i Sverige, oavsett var de personuppgiftsansvariga eller personuppgiftsbiträdena är etablerade (se kommentaren till 1 kap. 5 § tredje stycket). Bestämmelsen är inte tillämplig avseende barn som endast är på genomresa eller besök i landet. Det krävs däremot inte att barnet är folkbokfört i landet, att det redan har vistats i Sverige under en viss tidsperiod eller att det har beviljats uppehållstillstånd här för att det ska anses bo i Sverige. Även asylsökande barn i Sverige omfattas således av bestämmelsen.

Med informationssamhällets tjänster avses enligt artikel 4.25 i dataskyddsförordningen alla tjänster enligt definitionen i artikel 1.1 b i direktiv 2015/1535. I det direktivet definieras begreppet som tjänster som vanligtvis utförs mot ersättning på distans, på elektronisk väg och på individuell begäran av en tjänstemottagare. Det rör sig således om t.ex. sociala medier, söktjänster och s.k. appar på smarta enheter. Bestämmelsen är tillämplig när sådana tjänster erbjuds direkt till barn. Uttrycket direkt till barn ska tolkas och tillämpas på samma sätt som enligt dataskyddsförordningen. Det torde omfatta både tjänster som direkt marknadsförs mot barn och sådana tjänster vars utformning eller innehåll och funktion är av det slaget att de typiskt sett kan antas användas även av barn.

Om barnet är under 13 år, får behandling av personuppgifter ske antingen om samtycket ges av den person som har föräldraansvar för barnet eller om barnets samtycke godkänns av den personen. Begreppet den person som har föräldraansvar för barnet har samma innebörd som i dataskyddsförordningen. I första hand bör avses ett barns vårdnadshavare eller annan med uppdrag att vara i vårdnadshavarens ställe, t.ex. god man för ensamkommande barn. Eftersom begreppet är EU-rättsligt är det ytterst EU-domstolen som avgör begreppets innebörd. Det kan tänkas att begreppet har en vidare innebörd och även omfattar andra än vårdnadshavare, exempelvis föräldrar med umgängesrätt (jfr artikel 2.7 i Bryssel-II förordningen).

Rättslig förpliktelse

2 § Personuppgifter får behandlas med stöd av artikel 6.1 c i EU:s dataskyddsförordning, om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna fullgöra en rättslig förpliktelse som följer av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning.

Paragrafen anger förutsättningarna för att en rättslig förpliktelse ska utgöra rättslig grund för behandling av personuppgifter. Paragrafen saknar motsvarighet i personuppgiftslagen. Övervägandena finns i avsnitt 8.3.

Bestämmelsen har sin grund i artikel 6.3 första stycket i dataskyddsförordningen. Enligt artikeln måste en rättslig förpliktelse vara fastställd i enlighet med unionsrätten eller den nationella rätten för att kunna läggas till grund för behandling av personuppgifter. Paragrafen är inte avsedd att

inskränka innebörden av dataskyddsförordningens reglering om rättslig grund, utan endast att ge vägledning för rättstillämpningen i Sverige.

I paragrafen tydliggörs att en rättslig förpliktelse utgör rättslig grund för behandling av personuppgifter enligt artikel 6.1 c i dataskyddsförordningen, om förpliktelsen följer av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning. Förpliktelsen måste alltså vara fastställd i enlighet med gällande rätt, men behöver inte framgå direkt av en författning. Som en följd av den svenska arbetsmarknadsmodellen kan en rättslig förpliktelse även följa av kollektivavtal. Vidare kan en rättslig förpliktelse enligt svensk rätt även följa av t.ex. regeringsbeslut, myndighetsbeslut eller dom. Uttrycket följer av lag eller annan författning omfattar även direkt tillämpliga EU-förordningar.

Vid bedömningen av om något följer av exempelvis en lagbestämmelse kan bl.a. förarbetsuttalanden, bestämmelsens syfte och den rättsliga kontext bestämmelsen befinner sig i behöva beaktas. Det är alltså inte bara lagtextens ordalydelse som är av relevans för att avgöra om något följer av lag. Den rättsliga förpliktelsen behöver inte heller återfinnas direkt i t.ex. en lag eller ett kollektivavtal. Det kan också vara fråga om förpliktelser som även har sin grund i särskilt reglerade avtal, såsom försäkringsavtal. I sådana avtal finns ofta förpliktelser som kan härledas från krav i t.ex. lag eller kollektivavtal och som inte bara gäller mellan avtalsparterna utan även mot tredje part och som förutsätter behandling av personuppgifter.

För att en behandling av personuppgifter ska vara tillåten enligt artikel 6.1 c måste den också vara nödvändig för att fullgöra den rättsliga förpliktelsen. Detta innebär inte ett krav på att behandlingsåtgärden ska vara oundgänglig. Behandlingen kan anses nödvändig och därmed tillåten enligt artikel 6, om behandlingen leder till effektivitetsvinster. Att behandlingen skulle kunna ske manuellt, dvs. utan tekniska hjälpmedel, medför därför normalt inte att automatisk behandling inte anses nödvändig.

Uppgift av allmänt intresse och myndighetsutövning

3 § Personuppgifter får behandlas med stöd av artikel 6.1 e i EU:s dataskyddsförordning, om behandlingen är nödvändig

1. för att utföra en uppgift av allmänt intresse som följer av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning, eller
2. som ett led i den personuppgiftsansvariges myndighetsutövning enligt lag eller annan författning.

Paragrafen anger förutsättningarna för att en uppgift av allmänt intresse och myndighetsutövning ska utgöra rättslig grund för behandling av personuppgifter. Paragrafen saknar motsvarighet i personuppgiftslagen. Övervägandena finns i avsnitt 8.4 och 8.5.

Bestämmelsen har sin grund i artikel 6.3 första stycket i dataskyddsförordningen där det anges att en uppgift av allmänt intresse respektive myndighetsutövning måste fastställas i enlighet med unionsrätten eller den nationella rätten för att kunna läggas till grund för behandling av personuppgifter. Paragrafen är inte avsedd att inskränka

innebörden av dataskyddsförordningens reglering om rättslig grund, utan endast att ge vägledning för rättstillämpningen i Sverige.

I paragrafen anges att personuppgifter får behandlas med stöd av artikel 6.1 e i dataskyddsförordningen om behandlingen är nödvändig. Detta innebär inte ett krav på att behandlingsåtgärden ska vara oundgänglig, se kommentaren till 2 §.

I *punkt 1* tydliggörs att en uppgift av allmänt intresse utgör en rättslig grund för behandling av personuppgifter enligt artikel 6.1 e i dataskyddsförordningen, om uppgiften följer av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning. Det är alltså inte tillräckligt att uppgiften är av allmänt intresse – uppgiften måste också vara fastställd i enlighet med gällande rätt.

I fråga om vad som kan behöva beaktas vid bedömningen av om en uppgift följer av exempelvis en lagbestämmelse, se kommentaren till 2 §. Detta innebär inte att uppgiften måste framgå direkt av en författning. Som en följd av den svenska arbetsmarknadsmodellen kan en uppgift av allmänt intresse även följa av kollektivavtal. Uppgifter av allmänt intresse kan enligt svensk rätt även följa av beslut som har meddelats med stöd av lag eller annan författning. Till exempel kan en sådan uppgift tilldelas en statlig myndighet eller ett statligt bolag genom ett regeringsbeslut. Formuleringen omfattar även uppgifter som med stöd av kommunallagen lämnas till kommunala myndigheter och kommunala bolag genom beslut i fullmäktige. Även privaträttsligt bedriven verksamhet av allmänt intresse omfattas av formuleringen, förutsatt att uppgiften följer av lag eller annan författning eller följer av kollektivavtal eller av beslut som meddelats med stöd av lag eller annan författning. Uttrycket lag eller annan författning omfattar även direkt tillämpliga EU-förordningar.

I *punkt 2* tydliggörs att myndighetsutövning utgör en rättslig grund för behandling av personuppgifter bara om myndighetsutövningen sker enligt lag eller annan författning. Begreppet myndighetsutövning ska tolkas och tillämpas på samma sätt som enligt dataskyddsförordningen. Det som i Sverige brukar anses som myndighetsutövning torde omfattas av begreppet. Om en författning ställer upp krav för att myndighetsutövning ska få ske, t.ex. att ett privat subjekt ska vara certifierat, måste det vara uppfyllt för att myndighetsutövningen ska anses ske enligt författningen och utgöra en grund för behandling av personuppgifter.

Enskilda arkiv

4 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om att personuppgiftsansvariga som inte omfattas av föreskrifter om arkiv får behandla personuppgifter för arkivändamål av allmänt intresse.

Den myndighet som regeringen bestämmer får även i enskilda fall besluta att sådana personuppgiftsansvariga får behandla personuppgifter för arkivändamål av allmänt intresse. Ett beslut får förenas med villkor.

Paragrafen innehåller bl.a. ett bemyndigande för regeringen eller den myndighet som regeringen bestämmer att meddela föreskrifter om behandling av personuppgifter för arkivändamål av allmänt intresse

utanför arkivlagstiftningens tillämpningsområde. Paragrafen saknar motsvarighet i personuppgiftslagen. Övervägandena finns i avsnitt 14.1.2.

Paragrafen har sin grund i artikel 6.3 första stycket i dataskyddsförordningen, som innebär att en uppgift av allmänt intresse utgör rättslig grund för behandling av personuppgifter endast om uppgiften är fastställd i enlighet med unionsrätten eller den nationella rätten.

Enligt *första stycket* får regeringen eller den myndighet som regeringen bestämmer meddela föreskrifter om att personuppgiftsansvariga som inte omfattas av föreskrifter om arkiv får behandla personuppgifter för arkivändamål av allmänt intresse. Med föreskrifter om arkiv avses sådana föreskrifter som säkerställer att arkiv som utgör en del av det svenska kulturarvet bevaras, hålls ordnade och vårdas. Sådana föreskrifter finns i arkivlagen och arkivförordningen samt i Riksarkivets och andra arkivmyndigheters föreskrifter. Även i t.ex. lagen om Svenska kyrkan finns sådana föreskrifter.

Befogenhet att behandla personuppgifter kan enligt *andra stycket* även fastställas i förvaltningsbeslut.

En förutsättning för att föreskrifter ska få meddelas eller beslut fattas är att den personuppgiftsansvariges arkivverksamhet är av allmänt intresse i dataskyddsförordningens mening. Föreskrifter eller beslut som meddelas enligt dessa bestämmelser innebär att den personuppgiftsansvarige erkänns ha befogenhet att bedriva sådan arkivverksamhet. Föreskrifterna eller beslutet utgör därmed, på motsvarande sätt som föreskrifter om arkiv, en fastställd rättslig grund för behandling av personuppgifter för arkivändamål av allmänt intresse. Beslut i enskilda fall får förenas med villkor såsom återkallelseförbehåll, tidsbegränsningar eller krav på återrapportering eller tekniska och organisatoriska åtgärder, om det behövs för att säkerställa att kraven i dataskyddsförordningen uppfylls.

3 kap. Vissa kategorier av personuppgifter

Känsliga personuppgifter

Arbetsrätt, social trygghet och socialt skydd

1 § Känsliga personuppgifter får behandlas med stöd av artikel 9.2 b i EU:s dataskyddsförordning, om behandlingen är nödvändig för att den personuppgiftsansvarige eller den registrerade ska kunna fullgöra sina skyldigheter och utöva sina särskilda rättigheter inom arbetsrätten och inom områdena social trygghet och socialt skydd.

Personuppgifter som behandlas med stöd av första stycket får lämnas ut till tredje part endast om det inom arbetsrätten eller inom områdena social trygghet och socialt skydd finns en skyldighet för den personuppgiftsansvarige att göra det eller om den registrerade uttryckligen har samtyckt till utlämnandet.

I paragrafen regleras när känsliga personuppgifter får behandlas inom arbetsrättens område samt inom områdena social trygghet och socialt skydd. Paragrafen motsvarar 16 § första stycket a och andra stycket PUL. Övervägandena finns i avsnitt 10.3.

Bestämmelsen har sin grund i artikel 9.2 b i dataskyddsförordningen. Paragrafen är inte avsedd att inskränka innebörden av dataskyddsförordningens reglering om behandling av känsliga personuppgifter inom

arbetsrättens område samt inom områdena social trygghet och socialt skydd.

Enligt *första stycket* får känsliga personuppgifter behandlas om behandlingen är nödvändig för att den personuppgiftsansvarige eller den registrerade ska kunna fullgöra sina skyldigheter och utöva sina särskilda rättigheter inom arbetsrätten och inom områdena social trygghet och socialt skydd. Vad som avses med känsliga personuppgifter anges i 1 kap. 1 § andra stycket, se kommentaren till den bestämmelsen. Att behandlingen ska vara nödvändig innebär inte ett krav på att behandlingsåtgärden ska vara oundgänglig, jfr kommentaren till 2 kap. 2 §.

Begreppen arbetsrätten och områdena social trygghet och socialt skydd är unionsrättsliga begrepp som ska tolkas EU-konformt. I stort sett alla skyldigheter och rättigheter för arbetsgivare beträffande de anställda och deras organisationer bör kunna omfattas av uttrycken, exempelvis behandling i samband med sjuklön och rehabilitering av arbetstagare. Även skyldigheter och rättigheter för fackliga organisationer i förhållande till arbetsgivare och deras organisationer bör innefattas.

I *andra stycket* begränsas möjligheterna att lämna ut personuppgifter som behandlas med stöd av första stycket. Sådana uppgifter får lämnas ut till tredje part endast om det inom arbetsrätten eller inom områdena social trygghet och socialt skydd finns en skyldighet för den personuppgiftsansvarige att göra det eller om den registrerade uttryckligen har samtyckt till utlämnandet. Med skyldighet att lämna ut uppgifter avses sådan skyldighet som den personuppgiftsansvarige har och som följer av författning, myndighetsbeslut eller avtal inom arbetsrättens område och inom områdena social trygghet och socialt skydd. Termen tredje part definieras i artikel 4.10 i dataskyddsförordningen som en fysisk eller juridisk person, offentlig myndighet, institution eller ett organ som inte är den registrerade, den personuppgiftsansvarige, personuppgiftsbiträdet eller de personer som under den personuppgiftsansvariges eller personuppgiftsbiträdets direkta ansvar är behöriga att behandla personuppgifterna. Detta innebär exempelvis att en arbetsgivares utlämnande av personuppgifter till en facklig organisation omfattas av kravet på skyldighet eller samtycke.

Bestämmelsen i andra stycket innebär ingen begränsning av allmänhetens rätt till tillgång till handlingar enligt tryckfrihetsförordningen, se 1 kap. 7 §.

Viktigt allmänt intresse

2 § Känsliga personuppgifter får behandlas av en myndighet med stöd av artikel 9.2 g i EU:s dataskyddsförordning

1. om uppgifterna har lämnats till myndigheten och behandlingen krävs enligt lag,
2. om behandlingen är nödvändig för handläggningen av ett ärende, eller
3. i enstaka fall, om behandlingen är nödvändig med hänsyn till ett viktigt allmänt intresse och inte innebär ett otillbörligt intrång i den registrerades personliga integritet.

Vid tillämpningen av första stycket 1 ska andra än myndigheter jämställas med myndigheter, i den utsträckning bestämmelserna om allmänna handlingar och

sekretess i tryckfrihetsförordningen och offentlighets- och sekretesslagen (2009:400) gäller i deras verksamhet.

Paragrafen anger att myndigheter och andra som omfattas av offentlighetsprincipen får behandla känsliga personuppgifter i vissa fall. Bestämmelsen i andra punkten motsvarar delvis 8 § PUF. Övervägandena finns i avsnitt 10.4.

Bestämmelserna har sin grund i artikel 9.2 g i dataskyddsförordningen. Paragrafen är inte avsedd att inskränka innebörden av dataskyddsförordningens reglering om behandling av känsliga personuppgifter som är nödvändig med hänsyn till ett viktigt allmänt intresse.

Av *första stycket* framgår att känsliga personuppgifter får behandlas av en myndighet under vissa förutsättningar. Vad som avses med känsliga personuppgifter anges i 1 kap. 1 § andra stycket, se kommentaren till den bestämmelsen. Med myndighet avses samtliga statliga och kommunala organ, utom riksdagen och de beslutande kommunala församlingarna. Organ som är organiserade i privaträttsliga former, t.ex. kommunala och statliga bolag, är inte myndigheter, även om de utövar offentlig makt.

Punkt 1 anger att känsliga personuppgifter får behandlas av en myndighet om uppgifterna har lämnats till myndigheten och behandlingen krävs enligt lag. Bestämmelsen klargör att det är tillåtet för myndigheter att utföra sådan behandling av känsliga personuppgifter som krävs i myndigheternas verksamhet som en direkt följd av framför allt offentlighets- och sekretesslagens och förvaltningslagens bestämmelser om hur allmänna handlingar ska hanteras, exempelvis genom krav på diarieföring och skyldighet att ta emot e-post. Behandling av känsliga personuppgifter med stöd av denna punkt får bara ske om uppgifterna har lämnats till myndigheten. Uppgifterna ska alltså antingen finnas i handlingar som definieras som inkomna enligt 2 kap. 6 § TF eller lämnas till myndigheten på annat sätt, t.ex. muntligen. Vidare ska själva behandlingen av uppgifterna utgöra ett krav enligt lag.

Av punkt 2 framgår att känsliga personuppgifter får behandlas av en myndighet, om behandlingen är nödvändig för handläggningen av ett ärende. Begreppen handläggning och ärende ska tolkas på samma sätt som enligt 1 § förvaltningslagen (2017:900). Begreppet handläggning innefattar alla åtgärder som en myndighet vidtar från det att ett ärende inleds till dess att det avslutas. Kännetecknande för ett ärende är att det regelmässigt avslutas genom ett uttalande från myndighetens sida som är avsett att få faktiska verkningar för en mottagare i det enskilda fallet. Ett ärende avslutas således genom ett beslut av något slag. Vid bedömningen av om en myndighets uttalande är att anse som ett beslut i denna mening är det uttalandets syfte och innehåll som är avgörande, inte dess yttre form. Av paragrafen framgår vidare att behandlingen måste vara nödvändig för handläggningen av ärendet. Detta innebär bl.a. att bara sådana uppgifter som behövs i ärendet får behandlas. Begreppet nödvändig innebär inte ett krav på att behandlingsåtgärden ska vara oundgänglig, jfr författningskommentaren till 2 kap. 2 §.

Punkt 3 anger att känsliga personuppgifter får behandlas av en myndighet i enstaka fall, om behandlingen är nödvändig med hänsyn till ett viktigt allmänt intresse och inte innebär ett otillbörligt intrång i den registrerades personliga integritet. Bestämmelsen möjliggör under vissa

omständigheter behandling av känsliga personuppgifter hos myndigheter då behandlingen varken sker med koppling till ett visst ärende eller krävs enligt annan lag. Bestämmelsen är således tillämplig i s.k. faktisk verksamhet hos myndigheter, dvs. i sådan förvaltningsverksamhet som inte utgör ärendehandläggning. Bestämmelsen gäller i enstaka fall, vilket innebär att den inte kan tillämpas slentrianmässigt i den löpande verksamheten. Begränsningen hindrar däremot inte att bestämmelsen tillämpas vid behandling av många personuppgifter samtidigt. Vidare krävs att den personuppgiftsansvarige, i det enskilda fallet, gör en bedömning av om behandlingen innebär ett otillbörligt intrång i den registrerades personliga integritet. Om behandlingen skulle innebära ett sådant intrång, får den inte ske enligt denna bestämmelse. För att avgöra om intrånget är otillbörligt måste myndigheten bedöma om behovet av att utföra behandlingen väger tyngre än de registrerades intresse av att behandlingen inte sker. Bedömningen av de registrerades intresse av att behandlingen inte sker bör utgå från det intresse av integritetsskydd som de registrerade typiskt sett har. Den personuppgiftsansvarige måste således inte göra en bedömning i förhållande till varje berörd individ. Vid bedömningen av intrånget i den enskildes personliga integritet ska vikt läggas vid bl.a. uppgifternas känslighet, behandlingens karaktär, den inställning de registrerade kan antas ha till behandlingen, den spridning uppgifterna kan komma att få och risken för vidarebehandling för andra ändamål än insamlingsändamålet.

I *andra stycket* anges att vid tillämpningen av första stycket första punkten ska andra än myndigheter jämställas med myndigheter, i den utsträckning bestämmelserna om allmänna handlingar och sekretess i tryckfrihetsförordningen och offentlighets- och sekretesslagen gäller i deras verksamhet. Bestämmelsen innebär att alla personuppgiftsansvariga vars verksamhet omfattas av offentlighetsprincipen får behandla känsliga personuppgifter, om uppgifterna har lämnats till dem och behandlingen krävs enligt lag.

3 § Vid behandling som sker enbart med stöd av 2 § är det förbjudet att utföra sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter.

Paragrafen begränsar möjligheterna att utföra sökningar som avslöjar känsliga personuppgifter. Paragrafen har ingen motsvarighet i personuppgiftslagen. Övervägandena finns i avsnitt 10.4.

Enligt bestämmelsen är det förbjudet att utföra sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter. Förbudet gäller då känsliga personuppgifter behandlas enbart med stöd av 2 §. Detta innebär att sökbegränsningen inte gäller vid behandling som sker med stöd av någon av de övriga bestämmelserna i detta kapitel eller i enlighet med bestämmelser i en registerförfattning. Sökbegränsningen är inte heller tillämplig om behandlingen av känsliga personuppgifter sker med direkt tillämpning av något av undantagen i artikel 9.2 i dataskyddsförordningen.

Sökbegränsningen omfattar alla tekniska åtgärder som innebär att uppgifter används för att strukturera eller systematisera information i syfte att få fram ett urval av personer grundat på känsliga personuppgifter.

Därmed förbjuds sökningar som görs för att få fram ett urval av personer som t.ex. har en viss politisk åsikt, religiös åskådning eller sexuell läggning. Däremot hindrar bestämmelsen inte sökningar som görs i ett annat syfte än att identifiera ett urval av individer, t.ex. för att utöva tillsyn, för att ta fram verksamhetsstatistik eller för registervård.

4 § Regeringen får meddela ytterligare föreskrifter om sådan behandling av känsliga personuppgifter som är nödvändig med hänsyn till ett viktigt allmänt intresse.

Paragrafen innehåller ett bemyndigande för regeringen att meddela ytterligare föreskrifter om sådan behandling av känsliga personuppgifter som är nödvändig med hänsyn till ett viktigt allmänt intresse. Paragrafen motsvarar delvis 20 § PUL. Övervägandena finns i avsnitt 10.4.

Hälso- och sjukvård och social omsorg

5 § Känsliga personuppgifter får behandlas med stöd av artikel 9.2 h i EU:s dataskyddsförordning, om behandlingen är nödvändig för

1. förebyggande hälso- och sjukvård och yrkesmedicin,
2. bedömningen av en arbetstagares arbetskapacitet,
3. medicinska diagnoser,
4. tillhandahållande av hälso- och sjukvård eller behandling,
5. social omsorg, eller
6. förvaltning av social omsorg, hälso- och sjukvårdstjänster samt deras system.

Behandling enligt första stycket får ske under förutsättning att kravet på tystnadsplikt i artikel 9.3 i EU:s dataskyddsförordning är uppfyllt.

I paragrafen anges förutsättningarna för att känsliga personuppgifter ska få behandlas på hälso- och sjukvårdsområdet samt inom social omsorg. Paragrafen motsvarar delvis 18 § PUL. Övervägandena finns i avsnitt 10.5.

Bestämmelsen har sin grund i artikel 9.2 h i dataskyddsförordningen. Paragrafen är inte avsedd att inskränka innebörden av dataskyddsförordningens reglering om behandling av känsliga personuppgifter på hälso- och sjukvårdsområdet samt inom social omsorg.

I *första stycket* anges de ändamål för vilka behandling av känsliga personuppgifter får ske. Vad som avses med känsliga personuppgifter anges i 1 kap. 1 § andra stycket, se kommentaren till den bestämmelsen. Att behandlingen ska vara nödvändig innebär inte ett krav på att behandlingsåtgärden ska vara oundgänglig, jfr författningskommentaren till 2 kap. 2 §. De tillåtna ändamålen motsvarar de som anges i artikel 9.2 h i dataskyddsförordningen och har en EU-rättslig innebörd. Någon saklig skillnad i förhållande till förordningen är inte avsedd.

Andra stycket erinrar om kravet på tystnadsplikt i artikel 9.3 i dataskyddsförordningen som innebär att behandling av personuppgifter för de ändamål som avses i första stycket enbart får ske av eller under ansvar av en person som omfattas av tystnadsplikt enligt unionsrätten eller nationell rätt.

Arkiv

6 § Känsliga personuppgifter får behandlas för arkivändamål av allmänt intresse med stöd av artikel 9.2 j i EU:s dataskyddsförordning, om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna följa föreskrifter om arkiv.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om att personuppgiftsansvariga som inte omfattas av föreskrifter om arkiv får behandla känsliga personuppgifter för arkivändamål av allmänt intresse.

Den myndighet som regeringen bestämmer får även i enskilda fall besluta att sådana personuppgiftsansvariga får behandla känsliga personuppgifter för arkivändamål av allmänt intresse. Ett beslut får förenas med villkor.

Paragrafen reglerar när behandling av känsliga personuppgifter får ske för arkivändamål av allmänt intresse. Paragrafen motsvarar delvis 8 § andra stycket första meningen PUL. Övervägandena finns i avsnitt 14.1.3.

Bestämmelsen har sin grund i artikel 9.2 j i dataskyddsförordningen. Paragrafen är inte avsedd att inskränka innebörden av dataskyddsförordningens reglering om behandling av känsliga personuppgifter för arkivändamål av allmänt intresse.

I *första stycket* tydliggörs att känsliga personuppgifter får behandlas för arkivändamål av allmänt intresse, om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna följa föreskrifter om arkiv. Detta gäller oavsett om personuppgifterna samlas in för arkivändamål av allmänt intresse eller om uppgifter som samlats in för andra ändamål vidarebehandlas för arkivändamål av allmänt intresse. Vad som avses med känsliga personuppgifter anges i 1 kap. 1 § andra stycket, se kommentaren till den bestämmelsen. Att behandlingen ska vara nödvändig innebär inte ett krav på att behandlingsåtgärden ska vara oundgänglig, jfr kommentaren till 2 kap. 2 §. Med föreskrifter om arkiv avses föreskrifter som säkerställer att sådana arkiv som utgör en del av det svenska kulturarvet bevaras, hålls ordnade och vårdas. Sådana föreskrifter finns i arkivlagen och arkivförordningen samt i Riksarkivets och andra arkivmyndigheters föreskrifter. Föreskrifter om arkiv finns även t.ex. i lagen om Svenska kyrkan. Bestämmelsen förtydligar att dataskyddsförordningen och lagen inte hindrar att myndigheter eller andra som omfattas av offentlighetsprincipen arkiverar och bevarar allmänna handlingar eller att arkivmaterial tas om hand av en arkivmyndighet.

I *andra stycket* bemyndigas regeringen eller den myndighet som regeringen bestämmer att meddela föreskrifter som tillåter att personuppgiftsansvariga som inte omfattas av föreskrifter om arkiv får behandla känsliga personuppgifter för arkivändamål av allmänt intresse.

Enligt *tredje stycket* får den myndighet som regeringen bestämmer även genom beslut i enskilda fall tillåta sådan behandling.

Föreskrifter eller beslut enligt andra och tredje styckena kan aktualiseras om en enskild arkivinstitution samlar in känsliga personuppgifter för arkivändamål av allmänt intresse. De kan också aktualiseras i fall där t.ex. ett företag eller en förening har samlat in känsliga uppgifter för andra ändamål, men vidarebehandlar uppgifterna för arkivändamål av allmänt intresse. Beslut i enskilda fall som tillåter behandling av känsliga

personuppgifter för arkivändamål av allmänt intresse får förenas med villkor, om det behövs för att uppfylla kraven enligt artikel 9.2 j på lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen. Sådana villkor kan t.ex. avse begränsningar av åtkomsten till de känsliga uppgifterna, krav på särskilda tekniska säkerhetsåtgärder eller någon annan åtgärd som bedöms lämplig och proportionerlig i det aktuella fallet.

Statistik

7 § Känsliga personuppgifter får behandlas med stöd av artikel 9.2 j i EU:s dataskyddsförordning, om behandlingen är nödvändig för statistiska ändamål och samhällsintresset av det statistikprojekt där behandlingen ingår klart väger över den risk för otillbörligt intrång i enskildas personliga integritet som behandlingen kan innebära.

I paragrafen regleras behandling av känsliga personuppgifter för statistiska ändamål. Paragrafen motsvarar 19 § andra stycket PUL. Övervägandena finns i avsnitt 14.2.

Bestämmelsen har sin grund i artikel 9.2 j i dataskyddsförordningen. Paragrafen är inte avsedd att inskränka innebörden av dataskyddsförordningens reglering om behandling av känsliga personuppgifter för statistiska ändamål.

Enligt paragrafen får behandling av känsliga personuppgifter som är nödvändig för statistiska ändamål ske, om samhällsintresset av det statistikprojekt där behandlingen ingår klart väger över den risk för otillbörligt intrång i enskildas personliga integritet som behandlingen kan innebära. Vad som avses med känsliga personuppgifter anges i 1 kap. 1 § andra stycket, se kommentaren till den bestämmelsen. Att behandlingen ska vara nödvändig innebär inte ett krav på att behandlingsåtgärden ska vara oundgänglig, jfr kommentaren till 2 kap. 2 §.

Det krävs för det första att behandlingen är nödvändig för statistiska ändamål. Vidare är den personuppgiftsansvarige skyldig att göra en avvägning mellan de motstående intressena. Avvägningen ska ske genom en helhetsbedömning av samtliga omständigheter. Vid denna bedömning bör beaktas bl.a. statistikprojektets samhällsintresse och behovet av personuppgifter i projektet. Den personuppgiftsansvarige måste också noga överväga möjligheten att i stället inhämta de registrerades samtycke. Vid bedömningen av intrånget i den enskildes personliga integritet ska vikt läggas vid sådana aspekter som uppgifternas känslighet, den inställning de registrerade kan antas ha till behandlingen, säkerheten vid behandlingen och risken för att uppgifterna sprids eller att enskilda personer skulle kunna identifieras i statistiken. Bestämmelsen bör tolkas och tillämpas på ett likartat sätt som 19 § andra stycket PUL. Praxis kring tillämpningen av bestämmelsen i personuppgiftslagen bör således vara vägledande.

Personuppgifter som rör lagöverträdelser

8 § Personuppgifter som avses i artikel 10 i EU:s dataskyddsförordning får behandlas av myndigheter.

Även andra än myndigheter får behandla sådana personuppgifter, om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna följa föreskrifter om arkiv.

Paragrafen reglerar behandling av personuppgifter som rör lagöverträdelser. Paragrafen motsvarar delvis 21 § första stycket PUL. Övervägandena finns i avsnitt 11 och 14.1.3.

I *första stycket* anges att myndigheter får behandla sådana personuppgifter som avses i artikel 10 i dataskyddsförordningen. De personuppgifter som avses i artikel 10 är personuppgifter som rör fällande domar i brottmål och överträdelser eller därmed sammanhängande säkerhetsåtgärder. Begreppet därmed sammanhängande säkerhetsåtgärder torde vara likvärdigt med straffprocessuella tvångsmedel.

I *andra stycket* anges att även andra än myndigheter får behandla sådana personuppgifter som avses i artikel 10 i dataskyddsförordningen, om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna följa föreskrifter om arkiv. Att behandlingen ska vara nödvändig innebär inte ett krav på att behandlingsåtgärden ska vara oundgänglig, jfr kommentaren till 2 kap. 2 §. Med föreskrifter om arkiv avses detsamma som i 2 kap. 4 § första stycket, se kommentaren till den bestämmelsen. Bestämmelsen innebär, tillsammans med 6 § första stycket och de direkt tillämpliga bestämmelserna i dataskyddsförordningen, att dataskyddsförordningen och lagen inte hindrar att ett de personuppgiftsansvariga som omfattas av offentlighetsprincipen arkiverar och bevarar allmänna handlingar.

9 § Regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om i vilka fall andra än myndigheter får behandla sådana personuppgifter som avses i artikel 10 i EU:s dataskyddsförordning.

Den myndighet som regeringen bestämmer får även i enskilda fall besluta att andra än myndigheter får behandla sådana uppgifter. Ett beslut får förenas med villkor.

Paragrafen innehåller bl.a. ett bemyndigande för regeringen eller den myndighet som regeringen bestämmer att meddela föreskrifter som tillåter andra än myndigheter att behandla personuppgifter som rör lagöverträdelser. Paragrafen motsvarar delvis 21 § tredje och fjärde styckena PUL. Övervägandena finns i avsnitt 11.

Bestämmelsen har sin grund i artikel 10 i dataskyddsförordningen.

Enligt *första stycket* får regeringen eller den myndighet som regeringen bestämmer meddela föreskrifter om i vilka fall andra än myndigheter får behandla personuppgifter som avses i artikel 10 i EU:s dataskyddsförordning. Sådana föreskrifter kan exempelvis reglera behandling på vissa områden eller för vissa ändamål.

Enligt *andra stycket* får den myndighet som regeringen bestämmer även meddela beslut i enskilda fall som tillåter sådan behandling. Det som ska bedömas är om behandlingen är tillåten enligt dataskyddsförordningen, t.ex. om det finns en tillämplig rättslig grund enligt artikel 6 och om behandlingen är förenlig med principerna i artikel 5. Tillstånd bör i så fall beviljas, men vid behov förenas med krav på särskilda skyddsåtgärder för de registrerades rättigheter och friheter.

Beslut kan vid behov även förenas med villkor såsom återkallelseförbehåll, tidsbegränsningar eller krav på återrapportering.

Personnummer och samordningsnummer

10 § Personnummer och samordningsnummer får behandlas utan samtycke endast när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl.

Paragrafen reglerar när personnummer och samordningsnummer får behandlas utan samtycke. Bestämmelsen motsvarar 22 § PUL. Övervägandena finns i avsnitt 12.

Bestämmelsen, som har sin grund i artikel 87 i dataskyddsförordningen, anger att personnummer och samordningsnummer får behandlas utan samtycke endast när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl. Med personnummer och samordningsnummer avses detsamma som i folkbokföringslagen (1991:481). Bestämmelsen innebär att en intresseavvägning mellan behovet av behandlingen och de integritetsrisker som den innebär ska göras. Omständigheter som bör tillmätas betydelse vid intresseavvägningen är exempelvis om det eftersträvade syftet med behandlingen kan uppnås på annat sätt, behandlingens omfattning och om den förutsätter samkörning av register. Som ett exempel på sådan behandling som är tillåten enligt bestämmelsen kan nämnas den behandling som sker vid hanteringen av allmänna handlingar enligt t.ex. offentlighets- och sekretesslagen eller arkivlagen. Bestämmelsen bör tolkas och tillämpas på ett likartat sätt som 22 § PUL. Praxis kring tillämpningen av bestämmelsen i personuppgiftslagen bör således vara vägledande.

11 § Regeringen får meddela ytterligare föreskrifter om i vilka fall behandling av personnummer och samordningsnummer är tillåten.

Paragrafen innehåller ett bemyndigande för regeringen att meddela föreskrifter som tillåter behandling av personnummer och samordningsnummer i andra fall än enligt 10 §. Bestämmelsen motsvarar delvis 50 § c PUL. Övervägandena finns i avsnitt 12.

Bestämmelsen har sin grund i artikel 87 i dataskyddsförordningen.

4 kap. Användningsbegränsningar

Arkiv

1 § Personuppgifter som behandlas enbart för arkivändamål av allmänt intresse får användas för att vidta åtgärder i fråga om den registrerade endast om det finns synnerliga skäl med hänsyn till den registrerades vitala intressen.

Första stycket hindrar inte myndigheter från att använda personuppgifter som finns i allmänna handlingar.

Vid tillämpningen av andra stycket ska andra än myndigheter jämställas med myndigheter, i den utsträckning bestämmelserna om allmänna handlingar och sekretess i tryckfrihetsförordningen och offentlighets- och sekretesslagen (2009:400) gäller i deras verksamhet.

Paragrafen fastställer begränsningar för hur arkiverade personuppgifter får användas. Paragrafen motsvarar delvis 9 § fjärde stycket PUL och delvis 8 § andra stycket andra meningen PUL. Övervägandena finns i avsnitt 14.1.4.

Första stycket, som har sin grund i artiklarna 6.2, 9.2 j och 89.1 i dataskyddsförordningen, förhindrar att personuppgifter som behandlas av den personuppgiftsansvarige enbart för arkivändamål av allmänt intresse används för att vidta åtgärder rörande den registrerade. Sådana åtgärder får dock vidtas om det finns synnerliga skäl med hänsyn till den registrerades vitala intressen. Användningsbegränsningen gäller alla typer av personuppgifter och inte bara känsliga sådana. Med vitala intressen avses intressen som är av avgörande betydelse för den registrerades liv. Bestämmelsen skulle t.ex. kunna aktualiseras om arkiverade uppgifter måste användas för att identifiera och kontakta personer som utan deras vetskap har exponerats för farliga ämnen. Det är den personuppgiftsansvarige som har att visa att det finns sådana omständigheter som utgör synnerliga skäl. För att undantaget från användningsbegränsningen ska aktualiseras krävs att den aktuella användningen inte är oförenlig med det ändamål för vilket uppgifterna ursprungligen samlades in. Bestämmelsen kan alltså inte tillämpas till stöd för en vidarebehandling som i sig är otillåten.

Enligt *andra stycket* gäller inte användningsbegränsningen i första stycket för myndigheters användning av personuppgifter i allmänna handlingar. Myndigheter kan alltså använda arkiverade uppgifter för att vidta åtgärder gentemot den registrerade, förutsatt att övriga bestämmelser i dataskyddsregleringen följs, bl.a. att vidarebehandlingen är förenlig med det ursprungliga ändamålet (artikel 5.1 b i dataskyddsförordningen).

Av *tredje stycket* framgår att undantaget från användningsbegränsningen gäller även för andra än myndigheter, i den mån offentlighetsprincipen och offentlighets- och sekretesslagen gäller i deras verksamhet.

Bestämmelsen bör tolkas och tillämpas på ett likartat sätt som 9 § fjärde stycket PUL och 8 § andra stycket andra meningen PUL. Praxis kring tillämpningen av bestämmelsen i personuppgiftslagen bör således vara vägledande.

Statistik

2 § Personuppgifter som behandlas enbart för statistiska ändamål får användas för att vidta åtgärder i fråga om den registrerade endast om det finns synnerliga skäl med hänsyn till den registrerades vitala intressen.

Paragrafen fastställer begränsningar för hur personuppgifter som behandlas för statistikändamål får användas. Paragrafen motsvarar delvis 9 § fjärde stycket PUL. Övervägandena finns i avsnitt 14.2.

Bestämmelsen, som har sin grund i artiklarna 6.2, 9.2 j och 89.1 i dataskyddsförordningen, förhindrar att personuppgifter som behandlas av den personuppgiftsansvarige enbart för statistiska ändamål används för att vidta åtgärder rörande den registrerade. Sådana åtgärder får dock vidtas om det finns synnerliga skäl med hänsyn till den registrerades

vitala intressen. Begränsningen gäller alla typer av personuppgifter och inte bara känsliga sådana. Med vitala intressen avses intressen som är av avgörande betydelse för den registrerades liv. Ett exempel är när ett statistikregister används för att varna de personer som har köpt en apparat som visar sig ha ett allvarligt och farligt fel. Det är den personuppgiftsansvarige som har att visa att det finns sådana omständigheter som utgör synnerliga skäl. För att det ska vara tillåtet att använda uppgifterna för att vidta åtgärder i fråga om den registrerade krävs också att användningen inte är oförenlig med det ändamål för vilket uppgifterna ursprungligen samlades in (se artikel 5.1 b i dataskyddsförordningen). Undantaget från användningsbegränsningen kan alltså inte tillämpas till stöd för en vidarebehandling som i sig är otillåten enligt dataskyddsförordningen.

Bestämmelsen utgör, till skillnad från vad som gäller enligt 1 §, en begränsning även av myndigheters möjligheter att använda personuppgifter i allmänna handlingar för att vidta åtgärder i fråga om den registrerade. I övrigt bör bestämmelsen tolkas och tillämpas på ett likartat sätt som 9 § fjärde stycket PUL. Praxis kring tillämpningen av bestämmelsen i personuppgiftslagen bör således vara vägledande.

5 kap. Begränsningar av vissa rättigheter och skyldigheter

Information och tillgång till personuppgifter

1 § Artiklarna 13–15 i EU:s dataskyddsförordning om information och tillgång till personuppgifter gäller inte sådana uppgifter som den personuppgiftsansvarige inte får lämna ut till den registrerade enligt lag eller annan författning eller enligt beslut som har meddelats med stöd av författning.

Om den personuppgiftsansvarige inte är en myndighet, gäller undantaget i första stycket även för uppgifter som hos en myndighet skulle ha varit sekretessbelagda enligt offentlighets- och sekretesslagen (2009:400).

Paragrafen föreskriver undantag från den registrerades rätt till information och tillgång till personuppgifter m.m. enligt dataskyddsförordningen. Paragrafen motsvarar 27 § PUL. Övervägandena finns i avsnitt 13.

Bestämmelsen har sin grund i artikel 23 i dataskyddsförordningen.

I *första stycket* anges att artiklarna 13–15 i dataskyddsförordningen om information och tillgång inte gäller uppgifter som den personuppgiftsansvarige inte får lämna ut till den registrerade enligt lag eller annan författning eller enligt beslut som har meddelats med stöd av författning. Begreppen lag och författning omfattar även direkt tillämpliga EU-förordningar. Bestämmelsen innebär att sådan sekretess eller tystnadsplikt gentemot den registrerade som har stöd i författning har företräde framför rätten att få information och tillgång till personuppgifter m.m. Sådan sekretess kan i vissa fall gälla enligt offentlighets- och sekretesslagen till skydd för andra enskilda eller till skydd för allmänna intressen. Motsvarande sekretess kan också gälla enligt författningar som reglerar tystnadsplikt inom den privata sektorn, t.ex. enligt rättegångsbalken för advokater och enligt skollagen. Med beslut som har meddelats med stöd av författning avses t.ex. beslut om utlämnande av uppgift med förbehåll enligt 10 kap. 14 § OSL.

Andra stycket innebär att en personuppgiftsansvarig som inte omfattas av offentlighets- och sekretesslagens tillämpningsområde får vägra att lämna ut information till den registrerade, om en bestämmelse i den lagen hade hindrat utlämnande till den registrerade om den personuppgiftsansvarige hade varit en myndighet. Det kan t.ex. röra sig om information som samlats in inför en facklig förhandling eller en domstolsprocess, om det kan antas att ett utlämnande av informationen skulle försämra den personuppgiftsansvariges ställning som part i förhandlingen eller rättegången (jfr 19 kap. 6 och 9 §§ OSL).

Bestämmelsen bör tolkas och tillämpas på ett likartat sätt som 27 § PUL. Praxis kring tillämpningen av bestämmelsen i personuppgiftslagen bör således vara vägledande.

2 § Artikel 15 i EU:s dataskyddsförordning om den registrerades rätt till tillgång gäller inte personuppgifter i löpande text som inte har fått sin slutliga utformning när begäran gjordes eller som utgör minnesanteckning eller liknande.

Undantaget i första stycket gäller inte om personuppgifterna

1. har lämnats ut till tredje part,
2. behandlas enbart för arkivändamål av allmänt intresse eller statistiska ändamål, eller
3. har behandlats under längre tid än ett år i löpande text som inte har fått sin slutliga utformning.

Paragrafen föreskriver undantag från den registrerades rätt till bekräftelse på om personuppgifter som rör honom eller henne behandlas och i så fall att få tillgång till personuppgifterna och viss ytterligare information. Bestämmelsen motsvarar i sak 26 § tredje stycket PUL. Övervägandena finns i avsnitt 13.

Bestämmelsen har sin grund i artikel 23 i dataskyddsförordningen.

Av *första stycket* framgår att artikel 15 i dataskyddsförordningen om den registrerades rätt till tillgång inte gäller personuppgifter i löpande text som inte har fått sin slutliga utformning när begäran gjordes eller som utgör minnesanteckning eller liknande. Bestämmelsen innebär att den personuppgiftsansvarige inte behöver söka fram och till den registrerade lämna ut personuppgifter som finns i arbetsmaterial i form av löpande text. Med löpande text avses information som inte har strukturerats så att sökning av personuppgifter underlättas. Med text som inte har fått sin slutliga utformning avses koncept, utkast och liknande. Text som är avsedd att ändras eller kompletteras löpande och således aldrig kommer att få någon slutlig utformning omfattas inte av undantaget. Med text som utgör minnesanteckning avses promemorior och liknande som har kommit till bara för att bereda ett ärende, jfr 2 kap. 9 § TF.

Undantaget i första stycket från rätten till tillgång till personuppgifter m.m. enligt dataskyddsförordningen begränsas genom *andra stycket*. *Punkt 1* innebär att rätten till tillgång ändå gäller, om den handling där personuppgifterna förekommer har lämnats ut till tredje part. Termen tredje part definieras i artikel 4.10 i dataskyddsförordningen som en fysisk eller juridisk person, offentlig myndighet, institution eller ett organ som inte är den registrerade, den personuppgiftsansvarige, personuppgiftsbiträdet eller de personer som under den personuppgiftsansvariges eller personuppgiftsbiträdets direkta ansvar är behöriga att behandla

personuppgifterna. *Punkt 2* innebär att rätten till tillgång omfattar personuppgifter som behandlas enbart för arkivändamål av allmänt intresse eller statistiska ändamål. Rätten till tillgång omfattar således t.ex. sådana utkast eller minnesanteckningar som har tagits om hand för arkivering, liksom uppgifter i löpande text som behandlas för statistiska ändamål. Med behandling för arkivändamål av allmänt intresse eller statistiska ändamål avses detsamma som i dataskyddsförordningen. Slutligen innebär *punkt 3* att personuppgifter som förekommer i löpande text som inte har fått sin slutliga utformning omfattas av rätten till tillgång, om behandlingen har pågått under längre tid än ett år. Minnesanteckningar, som normalt får sin slutliga utformning i samband med att de förs, omfattas däremot inte av punkt 3. Personuppgifter som förekommer i sådana handlingar omfattas således inte av rätten till tillgång, även om behandlingen pågått i mer än ett år, under förutsättning att inte någon av punkterna 1 eller 2 är tillämplig.

Bestämmelsen bör tolkas och tillämpas på ett likartat sätt som 26 § tredje stycket PUL. Praxis kring tillämpningen av bestämmelsen i personuppgiftslagen bör således vara vägledande.

Bemyndigande

3 § Regeringen får meddela ytterligare föreskrifter om begränsningar enligt artiklarna 23, 89.2 och 89.3 i EU:s dataskyddsförordning.

Paragrafen innehåller ett bemyndigande för regeringen att meddela föreskrifter med stöd av artiklarna 23, 89.2 och 89.3 i dataskyddsförordningen. Bestämmelsen motsvarar 8 a § PUL. Övervägandena finns i avsnitt 13.

Föreskrifter som meddelas med stöd av bemyndigandet kan begränsa tillämpningsområdet för vissa av de registrerades rättigheter och de personuppgiftsansvarigas skyldigheter som föreskrivs i dataskyddsförordningen. Förutsättningarna för att sådana begränsningar ska kunna föreskrivas anges i artikel 23 och, i fråga om behandling för vetenskapliga eller historiska forskningsändamål, statistiska ändamål och arkivändamål av allmänt intresse, i artikel 89.2 och 89.3.

6 kap. Tillsynsmyndighetens handläggning och beslut

Befogenheter

1 § De befogenheter som tillsynsmyndigheten har enligt artikel 58.1, 58.2 och 58.3 i EU:s dataskyddsförordning gäller vid tillsyn över att bestämmelserna i denna lag och andra föreskrifter som kompletterar EU:s dataskyddsförordning följs.

Första stycket innebär inte att tillsynsmyndigheten får ta ut sanktionsavgifter vid andra överträdelser än de som avses i artikel 83 i EU:s dataskyddsförordning.

Paragrafen handlar om tillsynsmyndighetens befogenheter och saknar motsvarighet i personuppgiftslagen. Övervägandena finns i avsnitt 17.3.2.

Av *första stycket* framgår att de befogenheter som tillsynsmyndigheten har enligt artikel 58.1, 58.2 och 58.3 i dataskyddsförordningen gäller vid

tillsyn över att bestämmelserna i lagen och andra föreskrifter som kompletterar förordningen följs. I artikel 58.1 regleras tillsynsmyndighetens utredningsbefogenheter, t.ex. att beordra den personuppgiftsansvarige eller personuppgiftsbiträdet att lämna den information som myndigheten behöver för att kunna fullgöra sina uppgifter samt att genomföra undersökningar i form av dataskyddstillsyn. I artikel 58.2 anges tillsynsmyndighetens korrigerande befogenheter, t.ex. att utfärda varningar och att förelägga om rättelse eller radering av personuppgifter. Av artikel 58.3 framgår att tillsynsmyndigheten har befogenhet att utfärda tillstånd och att ge råd, t.ex. att godkänna utkast till uppförandekoder eller bindande företagsbestämmelser.

Med föreskrifter som kompletterar dataskyddsförordningen avses föreskrifter som rör behandling av personuppgifter i sådan verksamhet där dataskyddsförordningen gäller. Föreskrifter som kompletterar dataskyddsförordningen förekommer främst inom den offentliga sektorn och kan fastställa mer specifika krav för den behandling av personuppgifter som sker hos en viss myndighet eller inom en viss verksamhet. Som exempel kan nämnas patientdatalagen, studiestödsdatalagen och utlänningsdatalagen.

I *andra stycket* anges att första stycket inte innebär att tillsynsmyndigheten får ta ut sanktionsavgifter vid andra överträdelser än de som avses i artikel 83 i dataskyddsförordningen. Av bestämmelserna i artikel 83.4, 83.5 och 83.6 framgår att sanktionsavgifter kan tas ut vid överträdelser av vissa artiklar i förordningen samt av nationella bestämmelser som antagits på grundval av kapitel IX i dataskyddsförordningen. Med stöd av kapitel IX kan medlemsstaterna anta bestämmelser om t.ex. behandling av nationella identifikationsnummer (artikel 87) och behandling i anställningsförhållanden (artikel 88). Paragrafen utvidgar således inte det sanktionerade området och ger inte tillsynsmyndigheten en vidare befogenhet att ta ut sanktionsavgifter än vad som framgår av artikel 58.2 i.

Ansökan hos allmän förvaltningsdomstol

2 § Om tillsynsmyndigheten anser att det finns synnerliga skäl, får den ansöka hos allmän förvaltningsdomstol om att en åtgärd enligt artikel 58.2 i EU:s dataskyddsförordning ska vidtas, i stället för att själv besluta om åtgärden.

Ansökan ska göras hos den förvaltningsrätt som är behörig att pröva ett överklagande av tillsynsmyndighetens beslut.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Paragrafen reglerar tillsynsmyndighetens möjlighet att i vissa fall ansöka hos domstol om att en tillsynsåtgärd ska vidtas. Paragrafen saknar motsvarighet i personuppgiftslagen. Övervägandena finns i avsnitt 17.3.5.

Bestämmelsen i *första stycket*, som har sin grund i artikel 58.5 i dataskyddsförordningen, innebär att tillsynsmyndigheten, i stället för att själv fatta beslut om en korrigerande tillsynsåtgärd enligt artikel 58.2, får ansöka hos förvaltningsrätten om att åtgärden ska vidtas. Ansökningsförfarandet är tillgängligt endast om tillsynsmyndigheten anser att det finns synnerliga skäl, vilket innebär att möjligheten är avsedd att

utnyttjas mycket restriktivt. Bestämmelsen är framför allt tillämplig när det finns skäl att ifrågasätta giltigheten av en unionsrättsakt som meddelats med stöd av dataskyddsförordningen, dvs. delegerade akter eller genomförandeakter som avses i kapitel X i dataskyddsförordningen. Tillsynsmyndigheten kan i en sådan situation inte själv lösa normkonflikten genom att inte tillämpa den delegerade akten eller genomförandeakten. I stället får myndigheten ansöka hos förvaltningsrätten om att en tillsynsåtgärd ska vidtas. Om domstolen i ett sådant mål delar tillsynsmyndighetens tvivel angående aktens giltighet, kan domstolen begära ett förhandsavgörande från EU-domstolen och därigenom få giltigheten prövad innan något beslut om åtgärden fattas.

Enligt *andra stycket* ska ansökan göras hos den förvaltningsrätt som är behörig att pröva överklaganden av tillsynsmyndighetens beslut.

Av *tredje stycket* framgår att prövningstillstånd krävs vid överklagande till kammarrätten.

Sanktionsavgifter

3 § Tillsynsmyndigheten får ta ut en sanktionsavgift av en myndighet vid överträdelser som avses i artikel 83.4, 83.5 och 83.6 i EU:s dataskyddsförordning, i den ursprungliga lydelsen. Då ska artikel 83.1, 83.2 och 83.3 i förordningen tillämpas.

Sanktionsavgiften ska bestämmas till högst 5 000 000 kronor vid överträdelser som avses i artikel 83.4 i EU:s dataskyddsförordning och till högst 10 000 000 kronor vid överträdelser som avses i artikel 83.5 och 83.6 i förordningen.

Paragrafen slår fast att sanktionsavgifter enligt dataskyddsförordningen kan tas ut även av myndigheter, och anger de övre beloppsgränser som gäller i sådana fall. Paragrafen har ingen motsvarighet i personuppgiftslagen. Övervägandena finns i avsnitt 16.2.

Bestämmelserna i paragrafen har sin grund i artikel 83.7 i dataskyddsförordningen, enligt vilken varje medlemsstat får reglera om och i vilken utsträckning det ska vara möjligt att besluta om administrativa sanktionsavgifter mot offentliga myndigheter och organ.

Bestämmelsen i *första stycket* innebär att tillsynsmyndigheten får ta ut en sanktionsavgift även av en myndighet vid överträdelser av dataskyddsförordningen samt att de allmänna villkor för påförande av sanktionsavgifter som anges i artikel 83.1–3 i förordningen då ska tillämpas. Med myndighet avses detsamma som i 3 kap. 2 §, se kommentaren till den paragrafen. Hänvisningen till dataskyddsförordningen i första stycket är statisk, dvs. avser den ursprungliga lydelsen av förordningen.

I *andra stycket* fastställs de beloppsgränser som gäller vid sanktionsavgifter mot myndigheter. Sanktionsavgiften ska bestämmas till högst 5 000 000 kronor vid överträdelser som avses i artikel 83.4 i dataskyddsförordningen. Vid överträdelser som avses i artikel 83.5 och 83.6 i förordningen ska avgiften bestämmas till högst 10 000 000 kronor.

4 § Tillsynsmyndigheten får ta ut en sanktionsavgift vid överträdelser av artikel 10 i EU:s dataskyddsförordning, i den ursprungliga lydelsen. Då ska

artikel 83.1, 83.2 och 83.3 i förordningen tillämpas. Avgiftens storlek ska bestämmas med tillämpning av artikel 83.5 i förordningen.

Paragrafen, som saknar motsvarighet i personuppgiftslagen, reglerar möjligheten att ta ut sanktionsavgifter vid överträdelser av artikel 10 i dataskyddsförordningen om behandling av personuppgifter som rör lagöverträdelser. Övervägandena finns i avsnitt 16.3.3.

Paragrafen har sin grund i artikel 84 i dataskyddsförordningen.

Bestämmelsen innebär att tillsynsmyndigheten får ta ut en sanktionsavgift även vid överträdelser av artikel 10 i dataskyddsförordningen om behandling av personuppgifter som rör fällande domar i brottmål och överträdelser eller därmed sammanhängande säkerhetsåtgärder. Vidare innebär bestämmelsen att artikel 83.1, 83.2 och 83.2 ska gälla vid beslut om sådana sanktionsavgifter och att den övre beloppsgränsen enligt artikel 83.5 i förordningen är tillämplig. Hänvisningen till dataskyddsförordningen i denna paragraf är statisk, dvs. avser den ursprungliga lydelsen av förordningen.

Enligt 3 kap. 8 § får myndigheter behandla personuppgifter som rör lagöverträdelser. Det blir därmed inte aktuellt att ta ut sanktionsavgifter av en myndighet enligt denna paragraf.

5 § En sanktionsavgift får inte beslutas, om den som avgiften ska tas ut av inte har fått tillfälle att yttra sig inom fem år från den dag då överträdelsen ägde rum.

Ett beslut om sanktionsavgift ska delges.

Paragrafen, som saknar motsvarighet i personuppgiftslagen, reglerar bl.a. den bortre tidsgränsen för när en sanktionsavgift får beslutas. Övervägandena finns i avsnitt 16.4.

Första stycket innebär att om kommunikation enligt förvaltningslagen med den som avgiften ska tas ut av inte har skett inom fem år från överträdelsen, får en sanktionsavgift inte tas ut. Bevisbördan för att kommunikation har skett ligger på tillsynsmyndigheten. Tidsfristen räknas från när den otillåtna eller felaktiga behandlingen ägde rum.

Av *andra stycket* framgår att ett beslut om sanktionsavgift ska delges. Det innebär att myndigheten ska använda sig av de metoder för delgivning som regleras i delgivningslagen för att säkerställa att den som beslutet gäller får del av underrättelsen.

6 § En sanktionsavgift tillfaller staten.

Paragrafen, som saknar motsvarighet i personuppgiftslagen, föreskriver att sanktionsavgifter ska tillfalla staten. Övervägandena finns i avsnitt 16.4.

7 § En sanktionsavgift ska betalas till den myndighet som regeringen bestämmer inom 30 dagar från det att beslutet om att ta ut avgiften har fått laga kraft eller inom den längre tid som anges i beslutet.

Om sanktionsavgiften inte betalas inom den tid som anges i första stycket, ska myndigheten lämna den obetalda avgiften för indrivning. Bestämmelser om indrivning finns i lagen (1993:891) om indrivning av statliga fordringar m.m. Vid indrivning får verkställighet ske enligt utsökningsbalken.

Paragrafen, som saknar motsvarighet i personuppgiftslagen, reglerar betalning och indrivning av sanktionsavgifter. Övervägandena finns i avsnitt 16.4.

8 § Regeringen får meddela ytterligare föreskrifter om sanktionsavgifter enligt EU:s dataskyddsförordning och denna lag.

Paragrafen innehåller ett bemyndigande för regeringen att meddela föreskrifter om sanktionsavgifter enligt dataskyddsförordningen och lagen. Övervägandena finns i avsnitt 16.4.

Föreskrifter som meddelas med stöd av bemyndigandet i denna paragraf ska avse sådana sanktionsavgifter som regleras i dataskyddsförordningen eller lagen. Bemyndigandet kan således inte läggas till grund för föreskrifter som utvidgar det sanktionerade området.

7 kap. Skadestånd och överklagande

Skadestånd

1 § Rätten till ersättning från den personuppgiftsansvarige eller personuppgiftsbiträdet enligt artikel 82 i EU:s dataskyddsförordning gäller vid överträdelser av bestämmelser i denna lag och andra föreskrifter som kompletterar EU:s dataskyddsförordning.

Paragrafen upplyser om rätten till skadestånd vid överträdelser av föreskrifter som kompletterar dataskyddsförordningen. Bestämmelsen saknar motsvarighet i personuppgiftslagen. Övervägandena finns i avsnitt 17.1.1.

Bestämmelsen har sin grund i artikel 82 i dataskyddsförordningen och i skäl 146 till förordningen.

I paragrafen anges att rätten till ersättning från den personuppgiftsansvarige eller personuppgiftsbiträdet enligt dataskyddsförordningen gäller vid överträdelser av bestämmelser i lagen och i andra föreskrifter som kompletterar dataskyddsförordningen. Med föreskrifter som kompletterar dataskyddsförordningen avses detsamma som i 6 kap. 1 §, se kommentaren till den paragrafen.

Överklagande av personuppgiftsansvariga myndigheters beslut

2 § Beslut enligt artiklarna 12.5 och 15–21 i EU:s dataskyddsförordning som har meddelats av en myndighet i egenskap av personuppgiftsansvarig får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

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

Paragrafen reglerar rätten att överklaga beslut som en personuppgiftsansvarig myndighet meddelar med anledning av att en registrerad utövar sina rättigheter enligt dataskyddsförordningen. Paragrafen motsvarar delvis 52 § PUL. Övervägandena finns i avsnitt 17.1.2.

Av *första stycket* framgår vilka bestämmelser i dataskyddsförordningen som kan föranleda överklagbara beslut, nämligen artiklarna 12.5 och 15–

21. Med myndighet avses detsamma som i 3 kap. 2 §, se kommentaren till den paragrafen.

I *andra stycket* anges att prövningstillstånd krävs vid överklagande till kammarrätten.

Enligt *tredje stycket* gäller rätten att överklaga inte sådana beslut som fattas av regeringen, Högsta domstolen, Högsta förvaltningsdomstolen eller Riksdagens ombudsmän.

Överklagande av tillsynsmyndighetens beslut

3 § Tillsynsmyndighetens beslut enligt EU:s dataskyddsförordning och enligt 6 kap. 3 och 4 §§ denna lag får överklagas till allmän förvaltningsdomstol. När ett beslut överklagas, är tillsynsmyndigheten motpart i domstolen.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Paragrafen, som reglerar rätten att överklaga tillsynsmyndighetens beslut, motsvarar i sak 51 § och 53 § andra stycket PUL. Övervägandena finns i avsnitt 17.5.

Bestämmelsen har sin grund i artikel 78.1 i dataskyddsförordningen.

Av *första stycket* framgår att tillsynsmyndighetens beslut enligt dataskyddsförordningen samt om sanktionsavgifter enligt lagen får överklagas till allmän förvaltningsdomstol. Vidare anges att tillsynsmyndigheten är motpart i domstolen när ett beslut överklagas.

Enligt *andra stycket* krävs prövningstillstånd vid överklagande till kammarrätten.

Överklagande av andra beslut

4 § Beslut enligt 2 kap. 4 § andra stycket, 3 kap. 6 § tredje stycket och 3 kap. 9 § andra stycket denna lag får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Paragrafen reglerar rätten att överklaga vissa beslut i enskilda fall. Övervägandena finns i avsnitt 17.5.

Av *första stycket* framgår att beslut i enskilda fall om att personuppgiftsansvariga som inte omfattas av föreskrifter om arkiv får behandla personuppgifter för arkivändamål av allmänt intresse samt om att andra än myndigheter får behandla personuppgifter som rör lagöverträdelser får överklagas till allmän förvaltningsdomstol.

Enligt *andra stycket* krävs prövningstillstånd vid överklagande till kammarrätten.

Överklagandeförbud

5 § Andra beslut enligt EU:s dataskyddsförordning eller denna lag än de som avses i 2–4 §§ och 6 kap. 2 § får inte överklagas.

Paragrafen, som innehåller ett förbud mot att överklaga andra beslut än de som anges i 2–4 §§ och 6 kap. 2 §, motsvarar i sak 53 § PUL. Övervägandena finns i avsnitt 17.1.2 och 17.5.

Bestämmelsen innebär att beslut om att meddela föreskrifter med stöd av bemyndigandena i lagen inte får överklagas. Vidare innebär bestäm-

melsen att beslut som personuppgiftsansvariga myndigheter fattar enligt dataskyddsförordningen inte får överklagas i andra fall än de som anges i 2 §.

Ikraftträdande- och övergångsbestämmelser

1. Denna lag träder i kraft den 25 maj 2018.
2. Genom lagen upphävs personuppgiftslagen (1998:204).
3. I stället för vad som sägs i 1 kap. 2 §, ska den upphävda lagen fortsätta att gälla i sådan verksamhet hos Försvarsmakten, Försvarets radioanstalt och Totalförsvarets rekryteringsmyndighet som inte omfattas av unionsrätten.
4. Den upphävda lagen gäller fortfarande vid sådan behandling av personuppgifter som avses i artikel 2.2 d i EU:s dataskyddsförordning, i den ursprungliga lydelsen.
5. Den upphävda lagen gäller fortfarande i den utsträckning som det i en annan lag eller en förordning finns bestämmelser som innehåller hänvisningar till den lagen.
6. Den upphävda lagen gäller fortfarande för överklagande av beslut som har meddelats med stöd av den lagen.
7. Bestämmelsen i 49 § den upphävda lagen gäller fortfarande för överträdelser som har skett före ikraftträdandet.
8. Beslut som har meddelats med stöd av 21 § fjärde stycket den upphävda lagen gäller fortfarande.

Lagen träder enligt bestämmelsen i *punkt 1* i kraft den 25 maj 2018, dvs. den dag då dataskyddsförordningen börjar tillämpas. Bestämmelsen hindrar inte att tillsynsmyndigheten, en personuppgiftsansvarig eller ett personuppgiftsbiträde innan dess vidtar de administrativa åtgärder som behövs för att dataskyddsförordningen och lagen ska kunna tillämpas i sin helhet från och med ikraftträdandet.

Av *punkt 2* framgår att personuppgiftslagen upphävs genom lagen.

Enligt *punkt 3* ska, i stället för vad som sägs i 1 kap. 2 §, personuppgiftslagen fortsätta att gälla i sådan verksamhet hos Försvarsmakten, Försvarets radioanstalt och Totalförsvarets rekryteringsmyndighet som inte omfattas av unionsrätten. Bestämmelsen innebär att dataskyddsförordningen och lagen inte ska tillämpas i sådan verksamhet. Bestämmelsen är av övergångskaraktär och ska upphävas i samband med att en anpassad lagstiftning om behandling av personuppgifter i denna verksamhet träder i kraft.

Enligt *punkt 4* ska personuppgiftslagen fortfarande gälla vid sådan behandling av personuppgifter som avses i artikel 2.2 d i dataskyddsförordningen. Den behandling som avses är behandling av personuppgifter som utförs av behöriga myndigheter i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, i vilket även ingår att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten. Sådan behandling är undantagen från dataskyddsförordningens tillämpningsområde och regleras i stället i det nya dataskyddsdirektivet. Bestämmelsen är av övergångskaraktär och ska upphävas i samband med att den lagstiftning som genomför det nya dataskyddsdirektivet träder i kraft.

Punkt 5 anger att personuppgiftslagen fortfarande gäller i den utsträckning som det i en annan lag eller en förordning finns bestämmelser som

innehåller hänvisningar till den lagen. Bestämmelsen innebär att personuppgiftslagen övergångsvis fortsätter att gälla, vid sidan av dataskyddsförordningen, i den utsträckning som det finns hänvisningar i specialförfattningar till personuppgiftslagen.

Enligt *punkt 6* gäller personuppgiftslagen fortfarande för överklagande av beslut som har meddelats med stöd av den lagen.

Bestämmelsen i *punkt 7* innebär att personuppgiftslagens straffbestämmelse fortfarande gäller för straffbelagda gärningar som har begåtts vid behandling som har upphört före den 25 maj 2018 men som inte har lagförts före ikraftträdandet av den nya lagen. Administrativa sanktionsavgifter enligt dataskyddsförordningen bör däremot inte tas ut för en sådan överträdelse, med hänsyn till förbudet enligt 2 kap. 10 § RF mot retroaktiv straff- och skattelagstiftning.

Slutligen ska enligt *punkt 8* sådana beslut i enskilda fall avseende behandling av personuppgifter om lagöverträdelser m.m. som har meddelats med stöd av 21 § fjärde stycket PUL fortfarande gälla. Sådana äldre beslut innebär således att det är tillåtet enligt svensk rätt att behandla personuppgifter som avses i artikel 10 i dataskyddsförordningen.

Övervägandena finns i avsnitt 18.

20.2 Förslaget till lag om ändring i offentlighets- och sekretesslagen (2009:400)

10 kap.

27 § Utöver vad som följer av 2, 3, 5 och 15–26 §§ 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.

Första stycket gäller inte i fråga om sekretess enligt 24 kap. 2 a och 8 §§, 25 kap. 1–8 §§, 26 kap. 1–6 §§, 29 kap. 1 och 2 §§, 31 kap. 1 § första stycket, 2 och 12 §§, 33 kap. 2 §, 36 kap. 3 § samt 40 kap. 2 och 5 §§.

Första stycket gäller inte heller om utlämnandet strider mot lag eller förordning.

Paragrafen reglerar utlämnande av uppgifter som omfattas av sekretess mellan myndigheter i fall då det saknas uttryckliga sekretessbrytande regler. Ändringen innebär att tredje styckets hänvisning till föreskrifter som har meddelats med stöd av personuppgiftslagen stryks. Övervägandena finns i avsnitt 15.4.

21 kap.

Behandling i strid med *dataskyddsregleringen*

7 § Sekretess gäller för personuppgift, om det kan antas att *uppgiften efter* ett utlämnande *kommer att* behandlas i strid med *Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförord-*

ning), i den ursprungliga lydelsen, eller lagen (2018:00) med kompletterande bestämmelser till EU:s dataskyddsförordning.

Paragrafen reglerar sekretess i fall där det kan antas att utlämnade uppgifter kommer att behandlas i strid med dataskyddsregleringen. Övervägandena finns i avsnitt 15.3.

Ändringen i paragrafen innebär dels ett förtydligande av att prövningen gäller den behandling som kommer att ske efter ett eventuellt utlämnande, dels att hänvisningen till personuppgiftslagen ersätts med en hänvisning till dataskyddsförordningen och dataskyddslagen. En konsekvens av att hänvisningen inte enbart avser nationell rätt är att utlämnanden till utländska mottagare som omfattas av dataskyddsförordningens tillämpningsområde också omfattas av sekretessbestämmelsen.

Hänvisningen till dataskyddsförordningen i denna paragraf är statisk, dvs. avser den ursprungliga lydelsen av förordningen.

4.5.2016 SV Europeiska unionens officiella tidning L 119/1

I

(Lagstiftningsakter)

FÖRORDNINGAR

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2016/679

av den 27 april 2016

om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)

(Text av betydelse för EES)

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 16,

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande ([1]),

med beaktande av Regionkommitténs yttrande ([2]),

i enlighet med det ordinarie lagstiftningsförfarandet ([3]), och

av följande skäl:

(1) Skyddet för fysiska personer vid behandling av personuppgifter är en grundläggande rättighet. Artikel 8.1 i Europeiska unionens stadga om de grundläggande rättigheterna (nedan kallad *stadgan*) och artikel 16.1 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget) föreskriver att var och en har rätt till skydd av de personuppgifter som rör honom eller henne.

(2) Principerna och reglerna för skyddet för fysiska personer vid behandling av deras personuppgifter bör, oavsett deras medborgarskap eller hemvist, respektera deras grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter. Avsikten med denna förordning är att bidra till att skapa ett område med frihet, säkerhet och rättvisa och en ekonomisk union, till ekonomiska och sociala framsteg, till förstärkning och konvergens av ekonomierna inom den inre marknaden samt till fysiska personers välbefinnande.

(3) Europaparlamentets och rådets direktiv 95/46/EG ([4]) syftar till att harmonisera skyddet av fysiska personers grundläggande rättigheter och friheter vid behandling av personuppgifter och att säkerställa det fria flödet av personuppgifter mellan medlemsstaterna.

([1]) EUT C 229, 31.7.2012, s. 90.
([2]) EUT C 391, 18.12.2012, s. 127.
([3]) Europaparlamentets ståndpunkt av den 12 mars 2014 (ännu ej offentliggjord i EUT) och rådets ståndpunkt vid första behandlingen av den 8 april 2016 (ännu ej offentliggjord i EUT). Europaparlamentets ståndpunkt av den 14 april 2016.
([4]) 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).

(4) Behandlingen av personuppgifter bör utformas så att den tjänar människor. Rätten till skydd av personuppgifter är inte en absolut rättighet; den måste förstås utifrån sin uppgift i samhället och vägas mot andra grundläggande rättigheter i enlighet med proportionalitetsprincipen. Denna förordning respekterar alla grundläggande rättigheter och iakttar de friheter och principer som erkänns i stadgan, såsom de fastställts i fördragen, särskilt skydd för privat- och familjeliv, bostad och kommunikationer, skydd av personuppgifter, tankefrihet, samvetsfrihet och religionsfrihet, yttrande- och informationsfrihet, näringsfrihet, rätten till ett effektivt rättsmedel och en opartisk domstol samt kulturell, religiös och språklig mångfald.

(5) Den ekonomiska och sociala integration som uppstått tack vare den inre marknaden har lett till en betydande ökning av de gränsöverskridande flödena av personuppgifter. Utbytet av personuppgifter mellan offentliga och privata aktörer, inbegripet fysiska personer, sammanslutningar och företag, över hela unionen har ökat. Nationella myndigheter i medlemsstaterna uppmanas i unionsrätten att samarbeta och utbyta personuppgifter för att vara i stånd att fullgöra sina uppdrag eller utföra arbetsuppgifter för en myndighet som finns i en annan medlemsstat.

(6) Den snabba tekniska utvecklingen och globaliseringen har skapat nya utmaningar vad gäller skyddet av personuppgifter. Omfattningen av insamling och delning av personuppgifter har ökat avsevärt. Tekniken gör det möjligt för både privata företag och offentliga myndigheter att i sitt arbete använda sig av personuppgifter i en helt ny omfattning. Allt fler fysiska personer gör sina personliga uppgifter allmänt tillgängliga, världen över. Tekniken har omvandlat både ekonomin och det sociala livet, och bör ytterligare underlätta det fria flödet av personuppgifter inom unionen samt överföringar till tredjeländer och internationella organisationer, samtidigt som en hög skyddsnivå säkerställs för personuppgifter.

(7) Dessa förändringar kräver en stark och mer sammanhängande ram för dataskyddet inom unionen, uppbackad av kraftfullt tillsynsarbete, eftersom det är viktigt att skapa den tillit som behövs för att utveckla den digitala ekonomin över hela den inre marknaden. Fysiska personer bör ha kontroll över sina egna personuppgifter. Den rättsliga säkerheten och smidigheten för fysiska personer, ekonomiska operatörer och myndigheter bör stärkas.

(8) Om denna förordning föreskriver förtydliganden eller begränsningar av dess bestämmelser genom medlemsstaternas nationella rätt, kan medlemsstaterna, i den utsträckning det är nödvändigt för samstämmigheten och för att göra de nationella bestämmelserna begripliga för de personer som de tillämpas på, införliva delar av denna förordning i nationell rätt.

(9) Målen och principerna för direktiv 95/46/EG är fortfarande giltiga, men det har inte kunnat förhindra bristande enhetlighet i genomförandet av dataskyddet i olika delar av unionen, rättsosäkerhet eller allmänt spridda uppfattningar om att betydande risker kvarstår för fysiska personer, särskilt med avseende på användning av internet. Skillnader i nivån på skyddet av fysiska personers rättigheter och friheter, särskilt rätten till skydd av personuppgifter, vid behandling av personuppgifter i olika medlemsstater kan förhindra det fria flödet av personuppgifter över hela unionen. Dessa skillnader kan därför utgöra ett hinder för att bedriva ekonomisk verksamhet på unionsnivå, de kan snedvrida konkurrensen och hindra myndigheterna att fullgöra sina skyldigheter enligt unionsrätten. De varierande skyddsnivåerna beror på skillnader i genomförandet och tillämpningen av direktiv 95/46/EG.

(10) För att säkra en enhetlig och hög skyddsnivå för fysiska personer och för att undanröja hindren för flödena av personuppgifter inom unionen bör nivån på skyddet av fysiska personers rättigheter och friheter vid behandling av personuppgifter vara likvärdig i alla medlemsstater. En konsekvent och enhetlig tillämpning av bestämmelserna om skydd av fysiska personers grundläggande rättigheter och friheter vid behandling av personuppgifter bör säkerställas i hela unionen. Vad gäller behandlingen av personuppgifter för att fullgöra en rättslig förpliktelse, för att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning som utförs av den personuppgiftsansvarige, bör medlemsstaterna tillåtas att behålla eller införa nationella bestämmelser för att närmare fastställa hur bestämmelserna i denna förordning ska tillämpas. Jämte den allmänna och övergripande lagstiftning om dataskydd varigenom direktiv 95/46/EG genomförs har medlemsstaterna flera sektorsspecifika lagar på områden som kräver mer specifika bestämmelser. Denna förordning ger dessutom medlemsstaterna handlingsutrymme att specificera sina bestämmelser, även för behandlingen av särskilda kategorier av personuppgifter (nedan kallade *känsliga uppgifter*). Denna förordning utesluter inte att det i medlemsstaternas nationella rätt fastställs närmare omständigheter för specifika situationer där uppgifter behandlas, inbegripet mer exakta villkor för laglig behandling av personuppgifter.

(11) Ett effektivt skydd av personuppgifter över hela unionen förutsätter att de registrerades rättigheter förstärks och specificeras och att de personuppgiftsansvarigas och personuppgiftsbiträdenas skyldigheter vid behandling av personuppgifter klargörs, samt att det finns likvärdiga befogenheter för övervakning och att det säkerställs att reglerna för skyddet av personuppgifter efterlevs och att sanktionerna för överträdelser är likvärdiga i medlemsstaterna.

(12) I artikel 16.2 i EUF-fördraget bemyndigas Europaparlamentet och rådet att fastställa bestämmelser om skydd för fysiska personer när det gäller behandling av personuppgifter och bestämmelser om den fria rörligheten för personuppgifter.

(13) För att säkerställa en enhetlig nivå för skyddet av fysiska personer över hela unionen och undvika avvikelser som hindrar den fria rörligheten av personuppgifter inom den inre marknaden behövs en förordning som skapar rättslig säkerhet och öppenhet för ekonomiska aktörer, däribland mikroföretag samt små och medelstora företag, och som ger fysiska personer i alla medlemsstater samma rättsligt verkställbara rättigheter och skyldigheter samt ålägger personuppgiftsansvariga och personuppgiftsbiträden samma ansvar, så att övervakningen av behandling av personuppgifter blir enhetlig, sanktionerna i alla medlemsstater likvärdiga och samarbetet mellan tillsynsmyndigheterna i olika medlemsstater effektivt. För att den inre marknaden ska fungera väl krävs att det fria flödet av personuppgifter inom unionen inte begränsas eller förbjuds av skäl som har anknytning till skydd för fysiska personer med avseende på behandling av personuppgifter. För att ta hänsyn till mikroföretagens samt de små och medelstora företagens särskilda situation innehåller denna förordning ett undantag för organisationer som sysselsätter färre än 250 personer med avseende på registerföring. Dessutom uppmanas unionens institutioner och organ samt medlemsstaterna och deras tillsynsmyndigheter att vid tillämpningen av denna förordning ta hänsyn till mikroföretagens samt de små och medelstora företagens särskilda behov. Begreppen mikroföretag samt små och medelstora företag bör bygga på artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG ([1]).

(14) Det skydd som ska tillhandahållas enligt denna förordning bör tillämpas på fysiska personer, oavsett medborgarskap eller hemvist, med avseende på behandling av deras personuppgifter. Denna förordning omfattar inte behandling av personuppgifter rörande juridiska personer, särskilt företag som bildats som juridiska personer, exempelvis uppgifter om namn på och typ av juridisk person samt kontaktuppgifter.

(15) För att förhindra att det uppstår en allvarlig risk för att reglerna kringgås bör skyddet för fysiska personer vara teknikneutralt och inte vara beroende av den teknik som används. Skyddet för fysiska personer bör vara tillämpligt på både automatiserad och manuell behandling av personuppgifter, om personuppgifterna ingår i eller är avsedda att ingå i ett register. Akter eller grupper av akter samt omslag till dessa, som inte är ordnade enligt särskilda kriterier, bör inte omfattas av denna förordning.

(16) Denna förordning är inte tillämplig på frågor som rör skyddet av grundläggande rättigheter och friheter eller det fria flödet av personuppgifter på områden som inte omfattas av unionsrätten, såsom verksamhet rörande nationell säkerhet. Denna förordning är inte tillämplig på medlemsstaternas behandling av personuppgifter när de agerar inom ramen för unionens gemensamma utrikes- och säkerhetspolitik.

(17) Europaparlamentets och rådets förordning (EG) nr 45/2001 ([2]) är tillämplig på den behandling av personuppgifter som sker i unionens institutioner, organ och byråer. Förordning (EG) nr 45/2001 och de av unionens övriga rättsakter som är tillämpliga på sådan behandling av personuppgifter bör anpassas till principerna och bestämmelserna i den här förordningen och tillämpas mot bakgrund av den här förordningen. För att tillhandahålla en stark och sammanhängande ram för dataskyddet inom unionen bör nödvändiga anpassningar av förordning (EG) nr 45/2001 göras när den här förordningen har antagits, så att de båda förordningarna kan tillämpas samtidigt.

(18) Denna förordning är inte tillämplig på fysiska personers behandling av personuppgifter som ett led i verksamhet som är helt och hållet privat eller har samband med personens hushåll och därmed saknar koppling till yrkes- eller affärsmässig verksamhet. Privat verksamhet eller verksamhet som har samband med hushållet kan omfatta

([1]) Kommissionens rekommendation av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag (K(2003) 1422) (EUT L 124, 20.5.2003, s. 36).

([2]) Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter (EGT L 8, 12.1.2001, s. 1).

korrespondens och innehav av adresser, aktivitet i sociala nätverk och internetverksamhet i samband med sådan verksamhet. Denna förordning är dock tillämplig på personuppgiftsansvariga eller personuppgiftsbiträden som tillhandahåller utrustning för behandling av personuppgifter för sådan privat verksamhet eller hushållsverksamhet.

(19) Skyddet för fysiska personer när det gäller behöriga myndigheters behandling av personuppgifter i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten och det fria flödet av sådana uppgifter, säkerställs på unionsnivå av en särskild unionsrättsakt. Därför bör denna förordning inte vara tillämplig på behandling av personuppgifter för dessa ändamål. Personuppgifter som myndigheter behandlar enligt denna förordning och som används för de ändamålen bör emellertid regleras genom en mer specifik unionsrättsakt, nämligen Europaparlamentets och rådets direktiv (EU) 2016/680 ([1]). Medlemsstaterna får anförtro behöriga myndigheter i den mening som avses i direktiv (EU) 2016/680 uppgifter som inte nödvändigtvis utförs för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten, så att behandlingen av personuppgifter för dessa andra ändamål, i den mån den omfattas av unionsrätten, omfattas av tillämpningsområdet för denna förordning.

Vad gäller dessa behöriga myndigheters behandling av personuppgifter för ändamål som omfattas av tillämpningsområdet för denna förordning, bör medlemsstaterna kunna bibehålla eller införa mer specifika bestämmelser för att anpassa tillämpningen av bestämmelserna i denna förordning. I sådana bestämmelser får det fastställas mer specifika krav för dessa behöriga myndigheters behandling av personuppgifter för dessa andra ändamål, med beaktande av respektive medlemsstats konstitutionella, organisatoriska och administrativa struktur. När privata organs behandling av personuppgifter omfattas av tillämpningsområdet för denna förordning, bör denna förordning ge medlemsstaterna möjlighet att, under särskilda villkor, i lag begränsa vissa skyldigheter och rättigheter, om en sådan begränsning utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle för att skydda särskilda viktiga intressen, däribland allmän säkerhet samt förebyggande, förhindrande, utredning, avslöjande och lagföring av brott eller verkställande av straffrättsliga påföljder eller skydd mot samt förebyggande och förhindrande av hot mot den allmänna säkerheten. Detta är exempelvis relevant i samband med bekämpning av penningtvätt eller verksamhet vid kriminaltekniska laboratorier.

(20) Eftersom denna förordning bland annat gäller för verksamhet inom domstolar och andra rättsliga myndigheter, skulle det i unionsrätt eller medlemsstaternas nationella rätt kunna anges vilken behandling och vilka förfaranden för behandling som berörs när det gäller domstolars och andra rättsliga myndigheters behandling av personuppgifter. Tillsynsmyndigheternas behörighet bör inte omfatta domstolars behandling av personuppgifter när detta sker inom ramen för domstolarnas dömande verksamhet, i syfte att säkerställa domstolsväsendets oberoende när det utför sin rättsskipande verksamhet, inbegripet när det fattar beslut. Det bör vara möjligt att anförtro tillsynen över sådan behandling av uppgifter till särskilda organ inom medlemsstaternas rättsväsen, vilka framför allt bör säkerställa efterlevnaden av bestämmelserna i denna förordning, främja domstolsväsendets medvetenhet om sina skyldigheter enligt denna förordning och hantera klagomål relaterade till sådan behandling av uppgifter.

(21) Denna förordning påverkar inte tillämpningen av Europaparlamentets och rådets direktiv 2000/31/EG ([2]), särskilt bestämmelserna om tjänstelevererande mellanhänders ansvar i artiklarna 12–15 i det direktivet. Syftet med det direktivet är att bidra till att den inre marknaden fungerar väl genom att säkerställa fri rörlighet för informationssamhällets tjänster mellan medlemsstaterna.

(22) All behandling av personuppgifter som sker inom ramen för arbetet på personuppgiftsansvarigas eller personuppgiftsbiträdens verksamhetsställen inom unionen bör ske i överensstämmelse med denna förordning, oavsett om behandlingen i sig äger rum inom unionen. Verksamhetsställe innebär det faktiska och reella utförandet av verksamhet med hjälp av en stabil struktur. Den rättsliga formen för en sådan struktur, oavsett om det är en filial eller ett dotterföretag med status som juridisk person, bör inte vara den avgörande faktorn i detta avseende.

([1]) Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF (se sidan 89 i detta nummer av EUT).

([2]) Europaparlamentets och rådets direktiv 2000/31/EG av den 8 juni 2000 om vissa rättsliga aspekter på informationssamhällets tjänster, särskilt elektronisk handel, på den inre marknaden ("Direktiv om elektronisk handel") (EGT L 178, 17.7.2000, s. 1).

(23) För att fysiska personer inte ska fråntas det skydd som denna förordning ger dem bör sådan behandling av personuppgifter om registrerade personer som befinner sig i unionen vilken utförs av en personuppgiftsansvarig eller ett personuppgiftsbiträde som inte är etablerad inom unionen omfattas av denna förordning, om behandlingen avser utbjudande av varor eller tjänster inom unionen till de registrerade, oavsett om detta är kopplat till en betalning. I syfte att avgöra om en personuppgiftsansvarig eller ett personuppgiftsbiträde erbjuder varor eller tjänster till registrerade som befinner sig i unionen bör man fastställa om det är uppenbart att den personuppgiftsansvarige eller personuppgiftsbiträdet avser att erbjuda tjänster till registrerade i en eller flera av unionens medlemsstater. Medan enbart åtkomlighet till den personuppgiftsansvariges, personuppgiftsbiträdets eller en mellanhands webbplats i unionen, till en e-postadress eller andra kontaktuppgifter eller användning av ett språk som allmänt används i det tredjeland där den personuppgiftsansvarige är etablerad inte är tillräckligt för att fastställa en sådan avsikt, kan faktorer som användning av ett språk eller en valuta som allmänt används i en eller flera medlemsstater med möjlighet att beställa varor och tjänster på detta andra språk, eller omnämnande av kunder eller användare som befinner sig i unionen, göra det uppenbart att den personuppgiftsansvarige avser att erbjuda varor eller tjänster till registrerade inom unionen.

(24) Den behandling av personuppgifter som avser registrerade som befinner sig i unionen som utförs av en personuppgiftsansvarig eller ett personuppgiftsbiträde som inte är etablerad i unionen bör också omfattas av denna förordning, om den hör samman med övervakningen av de registrerade personernas beteende när de befinner sig i unionen. För att avgöra huruvida en viss behandling kan anses övervaka beteendet hos registrerade, bör det fastställas om fysiska personer spåras på internet, och om personuppgifterna därefter behandlas med hjälp av teknik som profilerar fysiska personer, i synnerhet för att fatta beslut rörande honom eller henne eller för att analysera eller förutsäga hans eller hennes personliga preferenser, beteende och attityder.

(25) Om medlemsstaternas nationella rätt är tillämplig i kraft av folkrätten, bör denna förordning också vara tillämplig på personuppgiftsansvariga som inte är etablerade inom unionen, exempelvis i en medlemsstats diplomatiska beskickning eller konsulat.

(26) Principerna för dataskyddet bör gälla all information som rör en identifierad eller identifierbar fysisk person. Personuppgifter som har pseudonymiserats och som skulle kunna tillskrivas en fysisk person genom att kompletterande uppgifter används bör anses som uppgifter om en identifierbar fysisk person. För att avgöra om en fysisk person är identifierbar bör man beakta alla hjälpmedel, som t.ex. utgallring, som, antingen av den personuppgiftsansvarige eller av en annan person, rimligen kan komma att användas för att direkt eller indirekt identifiera den fysiska personen. För att fastställa om hjälpmedel med rimlig sannolikhet kan komma att användas för att identifiera den fysiska personen bör man beakta samtliga objektiva faktorer, såsom kostnader och tidsåtgång för identifiering, med beaktande av såväl tillgänglig teknik vid tidpunkten för behandlingen som den tekniska utvecklingen. Principerna för dataskyddet bör därför inte gälla för anonym information, nämligen information som inte hänför sig till en identifierad eller identifierbar fysisk person, eller för personuppgifter som anonymiserats på ett sådant sätt att den registrerade inte eller inte längre är identifierbar. Denna förordning berör därför inte behandling av sådan anonym information, vilket inbegriper information för statistiska ändamål eller forskningsändamål.

(27) Denna förordning gäller inte behandling av personuppgifter rörande avlidna personer. Medlemsstaterna får fastställa bestämmelser för behandlingen av personuppgifter rörande avlidna personer.

(28) Tillämpningen av pseudonymisering av personuppgifter kan minska riskerna för de registrerade som berörs och hjälpa personuppgiftsansvariga och personuppgiftsbiträden att fullgöra sina skyldigheter i fråga om dataskydd. Ett uttryckligt införande av *pseudonymisering* i denna förordning är inte avsett att utesluta andra åtgärder för dataskydd.

(29) För att skapa incitament för tillämpning av pseudonymisering vid behandling av personuppgifter bör åtgärder för pseudonymisering som samtidigt medger en allmän analys vara möjliga inom samma personuppgiftsansvarigs verksamhet, när den personuppgiftsansvarige har vidtagit de tekniska och organisatoriska åtgärder som är nödvändiga för att se till att denna förordning genomförs för berörd uppgiftsbehandling och att kompletterande uppgifter för tillskrivning av personuppgifterna till en specifik registrerad person förvaras separat. Den personuppgiftsansvarige som behandlar personuppgifterna bör ange behöriga personer inom samma personuppgiftsansvarigs verksamhet.

(30) Fysiska personer kan knytas till nätidentifierare som lämnas av deras utrustning, applikationer, verktyg och protokoll, t.ex. ip-adresser, kakor eller andra identifierare, som radiofrekvensetiketter. Detta kan efterlämna spår som, särskilt i kombination med unika identifierare och andra uppgifter som tas emot av servrarna, kan användas för att skapa profiler för fysiska personer och identifiera dem.

(31) Offentliga myndigheter som för sin myndighetsutövning mottar personuppgifter i enlighet med en rättslig förpliktelse, t.ex. skatte- och tullmyndigheter, finansutredningsgrupper, oberoende administrativa myndigheter eller finansmarknadsmyndigheter med ansvar för reglering och övervakning av värdepappersmarknader, bör inte betraktas som mottagare om de tar emot personuppgifter som är nödvändiga för utförandet av en särskild utredning av allmänt intresse, i enlighet med unionsrätten eller medlemstaternas nationella rätt. Offentliga myndigheters begäranden om att uppgifter ska lämnas ut ska alltid vara skriftliga och motiverade, läggas fram i enskilda fall och inte gälla hela register eller leda till att register kopplas samman. Dessa offentliga myndigheters behandling av personuppgifter bör ske i överensstämmelse med de bestämmelser för dataskydd som är tillämpliga på behandlingens ändamål.

(32) Samtycke bör lämnas genom en entydig bekräftande handling som innebär ett frivilligt, specifikt, informerat och otvetydigt medgivande från den registrerades sida om att denne godkänner behandling av personuppgifter rörande honom eller henne, som t.ex. genom en skriftlig, inklusive elektronisk, eller muntlig förklaring. Detta kan inbegripa att en ruta kryssas i vid besök på en internetsida, genom val av inställningsalternativ för tjänster på informationssamhällets område eller genom någon annan förklaring eller något annat beteende som i sammanhanget tydligt visar att den registrerade godtar den avsedda behandlingen av sina personuppgifter. Tystnad, på förhand ikryssade rutor eller inaktivitet bör därför inte utgöra samtycke. Samtycket bör gälla all behandling som utförs för samma ändamål. Om behandlingen tjänar flera olika syften, bör samtycke ges för samtliga syften. Om den registrerade ska lämna sitt samtycke efter en elektronisk begäran, måste denna vara tydlig och koncis och får inte onödigtvis störa användningen av den tjänst som den avser.

(33) Det är ofta inte möjligt att fullt ut identifiera syftet med en behandling av personuppgifter för vetenskapliga forskningsändamål i samband med insamlingen av uppgifter. Därför bör registrerade kunna ge sitt samtycke till vissa områden för vetenskaplig forskning, när vedertagna etiska standarder för vetenskaplig forskning iakttas. Registrerade bör ha möjlighet att endast lämna sitt samtycke till vissa forskningsområden eller delar av forskningsprojekt i den utsträckning det avsedda syftet medger detta.

(34) Genetiska uppgifter bör definieras som personuppgifter som rör en fysisk persons nedärvda eller förvärvade genetiska kännetecken, vilka framgår av en analys av ett biologiskt prov från den fysiska personen i fråga, framför allt kromosom-, DNA- eller RNA-analys eller av en annan form av analys som gör det möjligt att inhämta motsvarande information.

(35) Personuppgifter om hälsa bör innefatta alla de uppgifter som hänför sig till en registrerad persons hälsotillstånd som ger information om den registrerades tidigare, nuvarande eller framtida fysiska eller psykiska hälsotillstånd. Detta inbegriper uppgifter om den fysiska personen som insamlats i samband med registrering för eller tillhandahållande av hälso- och sjukvårdstjänster till den fysiska personen enligt Europaparlamentets och rådets direktiv 2011/24/EU ([1]), ett nummer, en symbol eller ett kännetecken som den fysiska personen tilldelats för att identifiera denne för hälso- och sjukvårdsändamål, uppgifter som härrör från tester eller undersökning av en kroppsdel eller kroppssubstans, däribland genetiska uppgifter och biologiska prov, och andra uppgifter om exempelvis sjukdom, funktionshinder, sjukdomsrisk, sjukdomshistoria, klinisk behandling eller den registrerades fysiologiska eller biomedicinska tillstånd, oberoende av källan, exempelvis från en läkare eller från annan sjukvårdspersonal, ett sjukhus, en medicinteknisk produkt eller ett diagnostiskt in vitro-test.

(36) Den personuppgiftsansvariges huvudsakliga verksamhetsställe i unionen bör vara den plats i unionen där den personuppgiftsansvarige har sin centrala förvaltning, såvida inte beslut om ändamålen och medlen för behandling av personuppgifter fattas vid ett annat av den personuppgiftsansvariges verksamhetsställen i unionen; i sådant fall

([1]) Europaparlamentets och rådets direktiv 2011/24/EU av den 9 mars 2011 om tillämpningen av patienträttigheter vid gränsöverskridande hälso- och sjukvård (EUT L 88, 4.4.2011, s. 45).

bör det andra verksamhetsstället anses vara det huvudsakliga verksamhetsstället. En personuppgiftsansvarigs huvudsakliga verksamhetsställe inom unionen bör avgöras med beaktande av objektiva kriterier och bör inbegripa den faktiska och reella ledning som fattar de huvudsakliga besluten vad avser ändamål och medel för behandlingen med hjälp av en stabil struktur. Detta kriterium bör inte vara avhängigt av om behandlingen av personuppgifter utförs på detta ställe. Att tekniska medel och teknik för behandling av personuppgifter eller behandlingsverksamhet finns och används visar i sig inte att det rör sig om ett huvudsakligt verksamhetsställe och utgör därför inte avgörande kriterier för ett huvudsakligt verksamhetsställe. Personuppgiftsbiträdets huvudsakliga verksamhetsställe bör vara den plats i unionen där denne har sin centrala förvaltning eller, om denne inte har någon central förvaltning inom unionen, den plats inom unionen där den huvudsakliga behandlingen sker. I fall som omfattar både en personuppgiftsansvarig och ett personuppgiftsbiträde bör den behöriga ansvariga tillsynsmyndigheten fortfarande vara tillsynsmyndigheten i den medlemsstat där den personuppgiftsansvarige har sitt huvudsakliga verksamhetsställe, men den tillsynsmyndighet som gäller för personuppgiftsbiträdet bör betraktas som en berörd tillsynsmyndighet och den tillsynsmyndigheten bör delta i det samarbetsförfarande som föreskrivs i denna förordning. Om utkastet till beslut endast gäller den personuppgiftsansvarige, bör tillsynsmyndigheterna i den eller de medlemsstater där personuppgiftsbiträdet har ett eller flera verksamhetsställen inte under några omständigheter betraktas som berörda tillsynsmyndigheter. Om behandlingen utförs av en koncern bör det kontrollerande företagets huvudsakliga verksamhetsställe betraktas som koncernens huvudsakliga verksamhetsställe, utom då behandlingens ändamål och de medel med vilka den utförs fastställs av ett annat företag.

(37) En koncern bör innefatta ett kontrollerande företag och de företag som detta företag kontrollerar (kontrollerade företag), varvid det kontrollerande företaget bör vara det företag som kan utöva ett dominerande inflytande på de övriga företagen i kraft av exempelvis ägarskap, finansiellt deltagande eller de bestämmelser som det regleras av eller befogenheten att införa regler som rör personuppgiftsskyddet. Ett företag med kontroll över behandlingen av personuppgifter vid företag som är underställda detta företag bör, tillsammans med dessa företag, anses utgöra en koncern.

(38) Barns personuppgifter förtjänar särskilt skydd, eftersom barn kan vara mindre medvetna om berörda risker, följder och skyddsåtgärder samt om sina rättigheter när det gäller behandling av personuppgifter. Sådant särskilt skydd bör i synnerhet gälla användningen av barns personuppgifter i marknadsföringssyfte eller för att skapa personlighets- eller användarprofiler samt insamling av personuppgifter med avseende på barn när tjänster som erbjuds direkt till barn utnyttjas. Samtycke från den person som har föräldraansvar över ett barn bör inte krävas för förebyggande eller rådgivande tjänster som erbjuds direkt till barn.

(39) Varje behandling av personuppgifter måste vara laglig och rättvis. Det bör vara klart och tydligt för fysiska personer hur personuppgifter som rör dem insamlas, används, konsulteras eller på annat sätt behandlas samt i vilken utsträckning personuppgifterna behandlas eller kommer att behandlas. Öppenhetsprincipen kräver att all information och kommunikation i samband med behandlingen av dessa personuppgifter är lättillgänglig och lättbegriplig samt att ett klart och tydligt språk används. Den principen gäller framför allt informationen till registrerade om den personuppgiftsansvariges identitet och syftet med behandlingen samt ytterligare information för att sörja för en rättvis och öppen behandling för berörda fysiska personer och deras rätt att erhålla bekräftelse på och meddelande om vilka personuppgifter rörande dem som behandlas. Fysiska personer bör göras medvetna om risker, regler, skyddsåtgärder och rättigheter i samband med behandlingen av personuppgifter och om hur de kan utöva sina rättigheter med avseende på behandlingen. De specifika ändamål som personuppgifterna behandlas för bör vara tydliga och legitima och ha bestämts vid den tidpunkt då personuppgifterna samlades in. Personuppgifterna bör vara adekvata, relevanta och begränsade till vad som är nödvändigt för de ändamål som de behandlas för. Detta kräver i synnerhet att det tillses att den period under vilken personuppgifterna lagras är begränsad till ett strikt minimum. Personuppgifter bör endast behandlas om syftet med behandlingen inte rimligen kan uppnås genom andra medel. För att säkerställa att personuppgifter inte sparas längre än nödvändigt bör den personuppgiftsansvarige införa tidsfrister för radering eller för regelbunden kontroll. Alla rimliga åtgärder bör vidtas för att rätta eller radera felaktiga uppgifter. Personuppgifter bör behandlas på ett sätt som säkerställer lämplig säkerhet och konfidentialitet för personuppgifterna samt förhindrar obehörigt tillträde till och obehörig användning av personuppgifter och den utrustning som används för behandlingen.

(40) För att behandling ska vara laglig bör personuppgifterna behandlas efter samtycke från den berörda registrerade eller på någon annan legitim grund som fastställts i lag, antingen i denna förordning eller i annan unionsrätt eller

medlemsstaternas nationella rätt enligt denna förordning, vilket inbegriper att de rättsliga skyldigheter som åligger den personuppgiftsansvarige måste fullgöras eller att ett avtal i vilket den registrerade är part måste genomföras eller att åtgärder på begäran av den registrerade måste vidtas innan avtalet ingås.

(41) När det i denna förordning hänvisas till en rättslig grund eller lagstiftningsåtgärd, innebär detta inte nödvändigtvis en lagstiftningsakt antagen av ett parlament, utan att detta påverkar krav som uppställs i den konstitutionella ordningen i den berörda medlemsstaten. En sådan rättslig grund eller lagstiftningsåtgärd bör dock vara tydlig och precis och dess tillämpning bör vara förutsägbar för personer som omfattas av den, i enlighet med rättspraxis vid Europeiska unionens domstol (nedan kallad *domstolen*) och Europeiska domstolen för de mänskliga rättigheterna.

(42) När behandling sker efter samtycke från registrerade, bör personuppgiftsansvariga kunna visa att de registrerade har lämnat sitt samtycke till behandlingen. I synnerhet vid skriftliga förklaringar som rör andra frågor bör det finnas skyddsåtgärder som säkerställer att de registrerade är medvetna om att samtycke ges och om hur långt samtycket sträcker sig. I enlighet med rådets direktiv 93/13/EEG ([1]) bör en förklaring om samtycke som den personuppgiftsansvarige i förväg formulerat tillhandahållas i en begriplig och lätt tillgänglig form, med användning av ett klart och tydligt språk och utan oskäliga villkor. För att samtycket ska vara informerat bör den registrerade känna till åtminstone den personuppgiftsansvariges identitet och syftet med den behandling för vilken personuppgifterna är avsedda. Samtycke bör inte betraktas som frivilligt om den registrerade inte har någon genuin eller fri valmöjlighet eller inte utan problem kan vägra eller ta tillbaka sitt samtycke.

(43) För att säkerställa att samtycket lämnas frivilligt bör det inte utgöra giltig rättslig grund för behandling av personuppgifter i ett särskilt fall där det råder betydande ojämlikhet mellan den registrerade och den personuppgiftsansvarige, särskilt om den personuppgiftsansvarige är en offentlig myndighet och det därför är osannolikt att samtycket har lämnats frivilligt när det gäller alla förhållanden som denna särskilda situation omfattar. Samtycke antas inte vara frivilligt om det inte medger att separata samtycken lämnas för olika behandlingar av personuppgifter, trots att detta är lämpligt i det enskilda fallet, eller om genomförandet av ett avtal – inbegripet tillhandahållandet av en tjänst – är avhängigt av samtycket, trots att samtycket inte är nödvändigt för ett sådant genomförande.

(44) Behandling bör vara laglig när den är nödvändig i samband med avtal eller när det finns en avsikt att ingå ett avtal.

(45) Behandling som grundar sig på en rättslig förpliktelse som åvilar den personuppgiftsansvarige eller behandling som krävs för att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning, bör ha en grund i unionsrätten eller i en medlemsstats nationella rätt. Denna förordning medför inte något krav på en särskild lag för varje enskild behandling. Det kan räcka med en lag som grund för flera behandlingar som bygger på en rättslig förpliktelse som åvilar den personuppgiftsansvarige eller om behandlingen krävs för att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning. Behandlingens syfte bör också fastställas i unionsrätten eller i medlemsstaternas nationella rätt. Därtill skulle man genom denna grund kunna ange denna förordnings allmänna villkor för laglig personuppgiftsbehandling och precisera kraven för att fastställa vem den personuppgiftsansvarige är, vilken typ av personuppgifter som ska behandlas, vilka registrerade som berörs, de enheter till vilka personuppgifterna får lämnas ut, ändamålsbegränsningar, lagringstid samt andra åtgärder för att tillförsäkra en laglig och rättvis behandling. Unionsrätten eller medlemsstaternas nationella rätt bör också reglera frågan huruvida en personuppgiftsansvarig som utför en uppgift av allmänt intresse eller som ett led i myndighetsutövning ska vara en offentlig myndighet eller någon annan fysisk eller juridisk person som omfattas av offentligrättslig lagstiftning eller, om detta motiveras av allmänintresset, vilket inbegriper hälso- och sjukvårdsändamål, såsom folkhälsa och socialt skydd och förvaltning av hälso- och sjukvårdstjänster, av civilrättslig lagstiftning, exempelvis en yrkesorganisation.

(46) Behandling av personuppgifter bör även anses laglig när den är nödvändig för att skydda ett intresse som är av avgörande betydelse för den registrerades eller en annan fysisk persons liv. Behandling av personuppgifter på

([1]) Rådets direktiv 93/13/EEG av den 5 april 1993 om oskäliga villkor i konsumentavtal (EGT L 95, 21.4.1993, s. 29).

grundval av en annan fysisk persons grundläggande intressen bör i princip endast äga rum om behandlingen inte uppenbart kan ha en annan rättslig grund. Vissa typer av behandling kan tjäna både viktiga allmänintressen och intressen som är av grundläggande betydelse för den registrerade, till exempel när behandlingen är nödvändig av humanitära skäl, bland annat för att övervaka epidemier och deras spridning eller i humanitära nödsituationer, särskilt vid naturkatastrofer eller katastrofer orsakade av människan.

(47) En personuppgiftsansvarigs berättigade intressen, inklusive intressena för en personuppgiftsansvarig till vilken personuppgifter får lämnas ut, eller för en tredje part, kan utgöra rättslig grund för behandling, på villkor att de registrerades intressen eller grundläggande rättigheter och friheter inte väger tyngre, med beaktande av de registrerades rimliga förväntningar till följd av förhållandet till den personuppgiftsansvarige. Ett sådant berättigat intresse kan till exempel finnas när det föreligger ett relevant och lämpligt förhållande mellan den registrerade och den personuppgiftsansvarige i sådana situationer som att den registrerade är kund hos eller arbetar för den personuppgiftsansvarige. Ett berättigat intresse kräver under alla omständigheter en noggrann bedömning, som inbegriper huruvida den registrerade vid tidpunkten för inhämtandet av personuppgifter och i samband med detta rimligen kan förvänta sig att en uppgiftsbehandling för detta ändamål kan komma att ske. Den registrerades intressen och grundläggande rättigheter skulle i synnerhet kunna väga tyngre än den personuppgiftsansvariges intressen, om personuppgifter behandlas under omständigheter där den registrerade inte rimligen kan förvänta sig någon ytterligare behandling. Med tanke på att det är lagstiftarens sak att genom lagstiftning tillhandahålla den rättsliga grunden för de offentliga myndigheternas behandling av personuppgifter, bör den rättsliga grunden inte gälla den behandling de utför som ett led i fullgörandet av sina uppgifter. Sådan behandling av personuppgifter som är absolut nödvändig för att förhindra bedrägerier utgör också ett berättigat intresse för berörd personuppgiftsansvarig. Behandling av personuppgifter för direktmarknadsföring kan betraktas som ett berättigat intresse.

(48) Personuppgiftsansvariga som ingår i en koncern eller institutioner som är underställda ett centralt organ kan ha ett berättigat intresse att överföra personuppgifter inom koncernen för interna administrativa ändamål, bland annat för behandling av kunders eller anställdas personuppgifter. De allmänna principerna för överföring av personuppgifter, inom en koncern, till företag i tredjeland påverkas inte.

(49) Behandling av personuppgifter utgör ett berättigat intresse för berörd personuppgiftsansvarig i den mån den är absolut nödvändig och proportionell för att säkerställa nät- och informationssäkerhet, dvs. förmågan hos ett nät eller ett informationssystem att vid en viss tillförlitlighetsnivå tåla olyckshändelser, olagliga handlingar eller illvilligt uppträdande som äventyrar tillgängligheten, autenticiteten, integriteten och konfidentialiteten hos lagrade eller överförda personuppgifter och säkerheten hos besläktade tjänster som tillhandahålls av – eller är tillgängliga via – dessa nät och system, av myndigheter, incidenthanteringsorganisationer (Cert), enheter för hantering av datasäkerhetsincidenter, tillhandahållare av elektroniska kommunikationsnät och kommunikationstjänster och tillhandahållare av säkerhetsteknik och säkerhetstjänster. Detta skulle t.ex. kunna innefatta att förhindra obehörigt tillträde till elektroniska kommunikationsnät och felaktig kodfördelning och att sätta stopp för överbelastningsattacker och skador på datasystem och elektroniska kommunikationssystem.

(50) Behandling av personuppgifter för andra ändamål än de för vilka de ursprungligen samlades in bör endast vara tillåten, när detta är förenligt med de ändamål för vilka personuppgifterna ursprungligen samlades in. I dessa fall krävs det inte någon annan separat rättslig grund än den med stöd av vilken insamlingen av personuppgifter medgavs. Om behandlingen är nödvändig för att fullgöra en uppgift av allmänt intresse eller som ett led i myndighetsutövning som den personuppgiftsansvarige har fått i uppgift att utföra, kan unionsrätten eller medlemsstaternas nationella rätt fastställa och närmare ange för vilka uppgifter och syften ytterligare behandling bör betraktas som förenlig och laglig. Ytterligare behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål bör betraktas som förenlig och laglig behandling av uppgifter. Den rättsliga grund för behandling av personuppgifter som återfinns i unionsrätten eller i medlemsstaternas nationella rätt kan också utgöra en rättslig grund för ytterligare behandling. För att fastställa om ett ändamål med den ytterligare behandlingen är förenligt med det ändamål för vilket personuppgifterna ursprungligen insamlades bör den personuppgiftsansvarige, efter att ha uppfyllt alla krav vad beträffar den ursprungliga behandlingens lagenlighet, bland annat beakta alla kopplingar mellan dessa ändamål och ändamålen med den avsedda ytterligare behandlingen, det sammanhang inom vilket personuppgifterna insamlats, särskilt de registrerades rimliga förväntningar till följd av förhållandet till den personuppgiftsansvarige i fråga om den

art, den planerade ytterligare behandlingens konsekvenser för de registrerade samt förekomsten av lämpliga skyddsåtgärder för både den ursprungliga och den planerade ytterligare behandlingen.

Om den registrerade har gett sitt medgivande eller behandlingen grundar sig på unionsrätten eller på medlemsstaternas nationella rätt som utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle i syfte att säkerställa i synnerhet viktiga mål av allmänt intresse, bör den personuppgiftsansvarige tillåtas att behandla personuppgifterna ytterligare, oavsett om detta är förenligt med ändamålen eller inte. Under alla omständigheter bör tillämpningen av principerna i denna förordning, särskilt informationen till den registrerade om dessa andra ändamål och om dennes rättigheter, inbegripet rätten att göra invändningar, säkerställas. Om den personuppgiftsansvarige anmäler möjliga brott eller hot mot den allmänna säkerheten och i enskilda fall eller i flera fall som rör samma brott eller hot mot den allmänna säkerheten överför dessa personuppgifter till en behörig myndighet, ska detta betraktas som att den personuppgiftsansvarige agerar i ett berättigat intresse. Sådan överföring i den personuppgiftsansvariges berättigade intresse eller ytterligare behandling av personuppgifter bör emellertid vara förbjuden, om behandlingen inte är förenlig med lagstadgad eller yrkesmässig tystnadsplikt eller annan bindande tystnadsplikt.

(51) Personuppgifter som till sin natur är särskilt känsliga med hänsyn till grundläggande rättigheterna och friheter bör åtnjuta särskilt skydd, eftersom behandling av sådana uppgifter kan innebära betydande risker för de grundläggande rättigheterna och friheterna. Dessa personuppgifter bör även inbegripa personuppgifter som avslöjar ras eller etniskt ursprung, varvid användningen av termen *ras* i denna förordning inte innebär att unionen godtar teorier som söker fastställa förekomsten av skilda människoraser. Behandling av foton bör inte systematiskt anses utgöra behandling av särskilda kategorier av personuppgifter, eftersom foton endast definieras som biometriska uppgifter när de behandlas med särskild teknik som möjliggör identifiering eller autentisering av en fysisk person. Sådana personuppgifter bör inte behandlas, såvida inte behandling medges i särskilda fall som fastställs i denna förordning, med beaktande av att det i medlemsstaternas lagstiftning får införas särskilda bestämmelser om dataskydd för att anpassa tillämpningen av bestämmelserna i denna förordning i syfte att fullgöra en rättslig skyldighet eller en uppgift av allmänt intresse eller som ett led i myndighetsutövning som den personuppgiftsansvarige har fått i uppgift att utföra. Utöver de särskilda kraven för sådan behandling, bör de allmänna principerna och andra bestämmelser i denna förordning tillämpas, särskilt när det gäller villkoren för laglig behandling. Undantag från det allmänna förbudet att behandla sådana särskilda kategorier av personuppgifter bör uttryckligen fastställas, bland annat om den registrerade lämnar sitt uttryckliga samtycke eller för att tillgodose specifika behov, i synnerhet när behandlingen utförs inom ramen för legitima verksamheter som bedrivs av vissa sammanslutningar eller stiftelser i syfte att göra det möjligt att utöva grundläggande friheter.

(52) Undantag från förbudet att behandla särskilda kategorier av personuppgifter bör även tillåtas om de föreskrivs i unionsrätten eller i medlemsstaternas nationella rätt och underkastas lämpliga skyddsåtgärder för att skydda personuppgifter och övriga grundläggande rättigheter, när allmänintresset motiverar detta, i synnerhet i fråga om behandling av personuppgifter inom ramen för arbetsrätt och sociallagstiftning, däribland pensioner, och för hälsosäkerhetsändamål, övervaknings- och varningssyften, förebyggande eller kontroll av smittsamma sjukdomar och andra allvarliga hot mot hälsan. Detta undantag får göras för hälsoändamål, inbegripet folkhälsa och förvaltningen av hälso- och sjukvårdstjänster, särskilt för att säkerställa kvalitet och kostnadseffektivitet i de förfaranden som används vid prövningen av ansökningar om förmåner och tjänster inom sjukförsäkringssystemet, eller för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål. Genom undantag bör man även tillåta behandling av sådana personuppgifter där så krävs för fastställande, utövande eller försvar av rättsliga anspråk, oavsett om detta sker inom ett domstolsförfarande eller inom ett administrativt eller ett utomrättsligt förfarande.

(53) Särskilda kategorier av personuppgifter som förtjänar ett mer omfattande skydd bör endast behandlas i hälsorelaterade syften om detta krävs för att uppnå dessa syften och gagnar fysiska personer och samhället i stort, särskilt inom ramen för förvaltningen av tjänster för hälso- och sjukvård och social omsorg och deras system, inbegripet behandling som utförs av förvaltningen och centrala nationella hälsovårdsmyndigheter av sådana uppgifter för syften som hör samman med kvalitetskontroll, information om förvaltningen samt allmän nationell och lokal tillsyn över hälso- och sjukvårdssystemet och systemet för social omsorg och säkerställande av kontinuitet inom hälso- och sjukvård och social omsorg samt gränsöverskridande hälso- och sjukvård eller hälsosäkerhet, syften som hör samman med övervakning samt varningssyften eller för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål som baseras på unionsrätten eller på medlemsstaternas nationella rätt, vilka måste ha ett syfte av allmänt intresse, samt studier som genomförs av allmänt intresse på folkhälsoområdet. Denna förordning bör därför innehålla harmoniserade villkor för behandling av särskilda kategorier av personuppgifter om hälsa, vad gäller särskilda behov, i synnerhet när behandlingen av uppgifterna utförs för vissa hälsorelaterade syften av personer som enligt lag är underkastade

yrkesmässig tystnadsplikt. Unionsrätten eller medlemsstaternas nationella rätt bör föreskriva särskilda och lämpliga åtgärder som skyddar fysiska personers grundläggande rättigheter och personuppgifter. Medlemsstaterna bör få behålla eller införa ytterligare villkor, även begränsningar, för behandlingen av genetiska eller biometriska uppgifter eller uppgifter om hälsa. Detta bör emellertid inte hindra det fria flödet av personuppgifter inom unionen, när villkoren tillämpas på gränsöverskridande behandling av sådana uppgifter.

(54) På folkhälsoområdet kan det bli nödvändigt att med hänsyn till ett allmänt intresse behandla särskilda kategorier av personuppgifter utan att den registrerades samtycke inhämtas. Sådan behandling bör förutsätta lämpliga och särskilda åtgärder för att skydda fysiska personers rättigheter och friheter. I detta sammanhang bör *folkhälsa* tolkas enligt definitionen i Europaparlamentets och rådets förordning (EG) nr 1338/2008 ([1]), nämligen alla aspekter som rör hälsosituationen, dvs. allmänhetens hälsotillstånd, inbegripet sjuklighet och funktionshinder, hälsans bestämningsfaktorer, hälso- och sjukvårdsbehov, resurser inom hälso- och sjukvården, tillhandahållande av och allmän tillgång till hälso- och sjukvård, utgifter för och finansiering av hälso- och sjukvården samt dödsorsaker. Sådan behandling av uppgifter om hälsa av allmänt intresse bör inte innebära att personuppgifter behandlas för andra ändamål av tredje part, exempelvis arbetsgivare eller försäkrings- och bankföretag.

(55) Myndigheters behandling av personuppgifter på officiellt erkända religiösa sammanslutningars vägnar i syften som fastställs i grundlag eller i folkrätten anses också grunda sig på ett allmänt intresse.

(56) Om det för att det demokratiska systemet ska fungera i samband med allmänna val är nödvändigt att politiska partier i vissa medlemsstater samlar in personuppgifter om fysiska personers politiska uppfattningar, får behandling av sådana uppgifter tillåtas med hänsyn till ett allmänt intresse, på villkor att lämpliga skyddsåtgärder fastställs.

(57) Om de personuppgifter som behandlas av en personuppgiftsansvarig inte gör det möjligt för denne att identifiera en fysisk person, bör den personuppgiftsansvarige inte vara tvungen att skaffa ytterligare information för att kunna identifiera den registrerade, om ändamålet endast är att följa någon av bestämmelserna i denna förordning. Den personuppgiftsansvarige bör dock inte vägra att ta emot kompletterande uppgifter som den registrerade lämnat som stöd för utövandet av sina rättigheter. Identifiering bör omfatta digital identifiering av en registrerad, till exempel genom en autentiseringsmekanism, exempelvis samma identifieringsinformation som används av den registrerade för att logga in på den nättjänst som tillhandahålls av den personuppgiftsansvarige.

(58) Öppenhetsprincipen kräver att all information som riktar sig till allmänheten eller till registrerade är kortfattad, lättåtkomlig och lättbegriplig samt utformad på ett tydligt och enkelt språk samt att man vid behov använder visualisering. Denna information kan ges elektroniskt, exempelvis på en webbplats, när den riktas till allmänheten. Detta är särskilt relevant i situationer där mängden olika aktörer och den tekniska komplexiteten gör det svårt för den registrerade att veta och förstå om personuppgifter som rör honom eller henne samlas in, vem som gör det och för vilket syfte, exempelvis i fråga om reklam på nätet. Eftersom barn förtjänar särskilt skydd, bör all information och kommunikation som riktar sig till barn utformas på ett tydligt och enkelt språk som barnet lätt kan förstå.

(59) Förfaranden bör fastställas som gör det lättare för registrerade att utöva sina rättigheter enligt denna förordning, inklusive mekanismer för att begära och i förekommande fall kostnadsfritt få tillgång till och erhålla rättelse eller radering av personuppgifter samt för att utöva rätten att göra invändningar. Den personuppgiftsansvarige bör också tillhandahålla hjälpmedel för elektroniskt ingivna framställningar, särskilt i fall då personuppgifter behandlas elektroniskt. Personuppgiftsansvariga bör utan onödigt dröjsmål och senast inom en månad vara skyldiga att besvara registrerades önskemål och lämna en motivering, om de inte avser att uppfylla sådana önskemål.

([1]) Europaparlamentets och rådets förordning (EG) nr 1338/2008 av den 16 december 2008 om gemenskapsstatistik om folkhälsa och hälsa och säkerhet i arbetet (EUT L 354, 31.12.2008, s. 70).

(60) Principerna om rättvis och öppen behandling fordrar att den registrerade informeras om att behandling sker och syftet med den. Den personuppgiftsansvarige bör till den registrerade lämna all ytterligare information som krävs för att säkerställa en rättvis och öppen behandling, med beaktande av personuppgiftsbehandlingens specifika omständigheter och sammanhang. Dessutom bör den registrerade informeras om förekomsten av profilering samt om konsekvenserna av sådan profilering. Om personuppgifterna samlas in från den registrerade, bör denne även informeras om huruvida han eller hon är skyldig att tillhandahålla personuppgifterna och om konsekvenserna om han eller hon inte lämnar dem. Denna information får tillhandahållas kombinerad med standardiserade symboler för att ge en överskådlig, begriplig, lättläst och meningsfull överblick över den planerade behandlingen. Om sådana symboler visas elektroniskt bör de vara maskinläsbara.

(61) Information om behandling av personuppgifter som rör den registrerade bör lämnas till honom eller henne vid den tidpunkt då personuppgifterna samlas in från den registrerade eller, om personuppgifterna erhålls direkt från en annan källa, inom en rimlig period, beroende på omständigheterna i fallet. Om personuppgifter legitimt kan lämnas ut till en annan mottagare, bör de registrerade informeras första gången personuppgifterna lämnas ut till denna mottagare. Om den personuppgiftsansvarige avser att behandla personuppgifter för ett annat ändamål än det för vilket uppgifterna insamlades, bör denne före ytterligare behandling informera den registrerade om detta andra syfte och lämna annan nödvändig information. Om personuppgifternas ursprung inte kan meddelas den registrerade på grund av att olika källor har använts, bör allmän information ges.

(62) Det är dock inte nödvändigt att införa någon skyldighet att tillhandahålla information, om den registrerade redan innehar denna information, om registreringen eller utlämnandet av personuppgifterna uttryckligen föreskrivs i lag eller om det visar sig vara omöjligt eller skulle medföra orimliga ansträngningar att tillhandahålla den registrerade informationen. Det sistnämnda skulle särskilt kunna vara fallet om behandlingen sker för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål. I detta avseende bör antalet registrerade, uppgifternas ålder och lämpliga skyddsåtgärder beaktas.

(63) Den registrerade bör ha rätt att få tillgång till personuppgifter som insamlats om denne samt på enkelt sätt och med rimliga intervall kunna utöva denna rätt, för att vara medveten om att behandling sker och kunna kontrollera att den är laglig. Detta innefattar rätten för registrerade att få tillgång till uppgifter om sin hälsa, exempelvis uppgifter i läkarjournaler med t.ex. diagnoser, undersökningsresultat, bedömningar av behandlande läkare och eventuella vårdbehandlingar eller interventioner. Alla registrerade bör därför ha rätt att få kännedom och underrättelse om framför allt orsaken till att personuppgifterna behandlas, om möjligt vilken tidsperiod behandlingen pågår, vilka som mottar personuppgifterna, bakomliggande logik i samband med automatisk behandling av personuppgifter och, åtminstone när behandlingen bygger på profilering, konsekvenserna av sådan behandling. Om möjligt bör den personuppgiftsansvarige kunna ge fjärråtkomst till ett säkert system genom vilket den registrerade kan få direkt åtkomst till sina personuppgifter. Denna rätt bör inte inverka menligt på andras rättigheter eller friheter, t.ex. affärshemligheter eller immateriell äganderätt och särskilt inte på upphovsrätt som skyddar programvaran. Resultatet av dessa överväganden bör dock inte bli att den registrerade förvägras all information. Om den personuppgiftsansvarige behandlar en stor mängd uppgifter om den registrerade, bör den personuppgiftsansvarige kunna begära att den registrerade lämnar uppgift om vilken information eller vilken behandling en framställan avser, innan informationen lämnas ut.

(64) Personuppgiftsansvariga bör vidta alla rimliga åtgärder för att kontrollera identiteten på en registrerad som begär tillgång, särskilt inom ramen för nättjänster och i fråga om nätidentifierare. Personuppgiftsansvariga bör inte behålla personuppgifter enbart för att kunna agera vid en potentiell begäran.

(65) Den registrerade bör ha rätt att få sina personuppgifter rättade och en *rätt att bli bortglömd*, om lagringen av uppgifterna strider mot denna förordning eller unionsrätten eller medlemsstaternas nationella rätt som den personuppgiftsansvarige omfattas av. En registrerad bör särskilt ha rätt att få sina personuppgifter raderade och kunna begära att dessa personuppgifter inte behandlas, om de inte längre behövs med tanke på de ändamål för vilka de samlats in eller på annat sätt behandlats, om en registrerad har återtagit sitt samtycke till behandling eller invänder mot behandling av personuppgifter som rör honom eller henne, eller om behandlingen av hans eller

hennes personuppgifter på annat sätt inte överensstämmer med denna förordning. Denna rättighet är särskilt relevant när den registrerade har gett sitt samtycke som barn, utan att vara fullständigt medveten om riskerna med behandlingen, och senare vill ta bort dessa personuppgifter, särskilt på internet. Den registrerade bör kunna utöva denna rätt även när han eller hon inte längre är barn. Ytterligare lagring av personuppgifterna bör dock vara laglig, om detta krävs för att utöva yttrandefrihet och informationsfrihet, för att uppfylla en rättslig förpliktelse, för att utföra en uppgift i av allmänt intresse eller som ett led i myndighetsutövning som anförtrotts den personuppgiftsansvarige, med anledning av ett allmänt intresse inom folkhälsoområdet, för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål eller för fastställande, utövande eller försvar av rättsliga anspråk.

(66) För att stärka ”rätten att bli bortglömd” i nätmiljön bör rätten till radering utvidgas genom att personuppgiftsansvariga som offentliggjort personuppgifter är förpliktigade att vidta rimliga åtgärder, däribland tekniska åtgärder, för att informera de personuppgiftsansvariga som behandlar dessa personuppgifter om att den registrerade har begärt radering av alla länkar till och kopior eller reproduktioner av dessa personuppgifter. I samband med detta bör den personuppgiftsansvarige vidta rimliga åtgärder, med beaktande av tillgänglig teknik och de hjälpmedel som står den personuppgiftsansvarige till buds, däribland tekniska åtgärder, för att informera de personuppgiftsansvariga som behandlar personuppgifterna om den registrerades begäran.

(67) Sätten att begränsa behandlingen av personuppgifter kan bland annat inbegripa att man tillfälligt flyttar de valda personuppgifterna till ett annat databehandlingssystem, gör de valda uppgifterna otillgängliga för användare eller tillfälligt avlägsnar offentliggjorda uppgifter från en webbplats. I automatiserade register bör begränsningen av behandlingen i princip ske med tekniska medel på ett sådant sätt att personuppgifterna inte blir föremål för ytterligare behandling och inte kan ändras. Det förhållandet att behandlingen av personuppgifter är begränsad bör klart anges inom systemet.

(68) För att ytterligare förbättra kontrollen över sina egna uppgifter bör den registrerade, om personuppgifterna behandlas automatiskt, också tillåtas att motta de personuppgifter som rör honom eller henne, som han eller hon har tillhandahållit den personuppgiftsansvarige, i ett strukturerat, allmänt använt, maskinläsbart och kompatibelt format och överföra dessa till en annan personuppgiftsansvarig. Personuppgiftsansvariga bör uppmuntras att utveckla kompatibla format som möjliggör dataportabilitet. Denna rättighet bör vara tillämplig om den registrerade har tillhandahållit uppgifterna efter att ha lämnat sitt samtycke eller om behandlingen är nödvändig för att ett avtal ska kunna genomföras. Den bör inte vara tillämplig om behandlingen utgår från en annan rättslig grund än samtycke eller avtal. På grund av sin art bör denna rättighet inte utövas mot personuppgiftsansvariga som behandlar personuppgifter som ett led i myndighetsutövning. Därför bör den inte vara tillämplig när behandlingen av personuppgifterna är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige eller för att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning som utförs av den personuppgiftsansvarige. Den registrerades rätt att överföra eller motta personuppgifter som rör honom eller henne innebär inte någon skyldighet för de personuppgiftsansvariga att införa eller upprätthålla behandlingssystem som är tekniskt kompatibla. Om mer än en registrerad berörs inom en viss uppsättning personuppgifter, bör rätten att motta personuppgifterna inte inverka på andra registrerades rättigheter och friheter enligt denna förordning. Denna rättighet bör inte heller påverka den registrerades rätt att få till stånd radering av personuppgifter och de inskränkningar av denna rättighet vilka anges i denna förordning och bör i synnerhet inte medföra radering av personuppgifter om den registrerade som denne har lämnat för genomförande av ett avtal, i den utsträckning och så länge som personuppgifterna krävs för genomförande av avtalet. Om det är tekniskt möjligt, bör den registrerade ha rätt till direkt överföring av personuppgifterna från en personuppgiftsansvarig till en annan.

(69) När personuppgifter lagligen får behandlas, eftersom behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i en myndighetsutövning som utförs av den personuppgiftsansvarige, eller på grund av en personuppgiftsansvarigs eller en tredje parts berättigade intressen, bör alla registrerade ändå ha rätt att göra invändningar mot behandling av personuppgifter som rör de registrerades särskilda situation. Det bör ankomma på den personuppgiftsansvarige att visa att dennes tvingande berättigade intressen väger tyngre än den registrerades intressen eller grundläggande rättigheter och friheter.

(70) Om personuppgifter behandlas för direktmarknadsföring, bör den registrerade, oavsett om det handlar om inledande eller ytterligare behandling, ha rätt att när som helst kostnadsfritt invända mot sådan behandling, inbegripet profilering, i den mån denna är kopplad till direktmarknadsföring. Denna rättighet bör uttryckligen meddelas den registrerade och redovisas tydligt, klart och åtskilt från annan information.

(71) Den registrerade bör ha rätt att inte bli föremål för ett beslut, vilket kan inbegripa en åtgärd, med bedömning av personliga aspekter rörande honom eller henne, vilket enbart grundas på automatiserad behandling och medför rättsverkan för honom eller henne eller på liknande sätt i betydande grad påverkar honom eller henne, såsom ett automatiserat avslag på en kreditansökan online eller e-rekrytering utan personlig kontakt. Sådan behandling omfattar ”profilering” i form av automatisk behandling av personuppgifter med bedömning av personliga aspekter rörande en fysisk person, särskilt för att analysera eller förutse aspekter avseende den registrerades arbetsprestation, ekonomiska situation, hälsa, personliga preferenser eller intressen, pålitlighet eller beteende, vistelseort eller förflyttningar, i den mån dessa har rättsverkan rörande honom eller henne eller på liknande sätt i betydande grad påverkar honom eller henne. Beslutsfattande grundat på sådan behandling, inbegripet profilering, bör dock tillåtas när det uttryckligen beviljas genom unionsrätten eller medlemsstaternas nationella rätt som den personuppgiftsansvarige omfattas av, inbegripet för sådan övervakning och sådant förebyggande av bedrägerier och skatteundandragande som genomförs i enlighet med unionsinstitutionernas eller de nationella tillsynsorganens bestämmelser, standarder och rekommendationer samt för att sörja för tillförlitlighet hos en tjänst som tillhandahålls av den personuppgiftsansvarige, eller när det krävs för ingående eller genomförande av ett avtal mellan den registrerade och en personuppgiftsansvarig eller den registrerade har gett sitt uttryckliga samtycke. Denna form av uppgiftsbehandling bör under alla omständigheter omgärdas av lämpliga skyddsåtgärder, som bör inkludera specifik information till den registrerade och rätt till mänskligt ingripande, att framföra sina synpunkter, att erhålla en förklaring till det beslut som fattas efter sådan bedömning och att överklaga beslutet. Sådana åtgärder bör inte gälla barn.

I syfte att sörja för rättvis och transparent behandling med avseende på den registrerade, med beaktande av omständigheterna och det sammanhang i vilket personuppgifterna behandlas, bör den personuppgiftsansvarige använda adekvata matematiska eller statistiska förfaranden för profilering, genomföra tekniska och organisatoriska åtgärder som framför allt säkerställer att faktorer som kan medföra felaktigheter i personuppgifter korrigeras och att risken för fel minimeras samt säkra personuppgifterna på sådant sätt att man beaktar potentiella risker för den registrerades intressen och rättigheter och förhindrar bland annat diskriminerande effekter för fysiska personer, på grund av ras eller etniskt ursprung, politiska åsikter, religion eller övertygelse, medlemskap i fackföreningar, genetisk status eller hälsostatus eller sexuell läggning, eller som leder till åtgärder som får sådana effekter. Automatiserat beslutsfattande och profilering baserat på särskilda kategorier av personuppgifter bör endast tillåtas på särskilda villkor.

(72) Profilering omfattas av denna förordnings bestämmelser om behandling av personuppgifter, såsom de rättsliga grunderna för behandlingen och principer för dataskydd. Europeiska dataskyddsstyrelsen som inrättas genom denna förordning (nedan kallad *styrelsen*) bör kunna utfärda riktlinjer i detta avseende.

(73) Begränsningar med avseende på specifika principer och rätten till information, tillgång till och rättelse eller radering av personuppgifter, rätten till dataportabilitet, rätten att göra invändningar, profileringsbaserade beslut samt information till den registrerade om personuppgiftsincidenter och vissa av den personuppgiftsansvariges relaterade skyldigheter kan införas genom unionsrätten eller medlemsstaternas nationella rätt, i den mån de är nödvändiga och proportionella i ett demokratiskt samhälle för att upprätthålla den allmänna säkerheten, exempelvis för att skydda människoliv, särskilt vid naturkatastrofer eller katastrofer framkallade av människan, vid förebyggande, förhindrande, utredning och lagföring av brott eller verkställande av straffrättsliga sanktioner, inbegripet skydd mot samt förebyggande och förhindrande av hot mot den allmänna säkerheten eller överträdelser av etiska principer för reglerade yrken, vad gäller unionens eller en medlemsstats övriga viktiga mål av allmänt intresse, särskilt om de är av stort ekonomiskt eller finansiellt intresse för unionen eller en medlemsstat, förande av offentliga register som förs av hänsyn till ett allmänt intresse, ytterligare behandling av arkiverade personuppgifter för att tillhandahålla specifik information om politiskt beteende under tidigare totalitära regimer eller skydd av den registrerade eller andras rättigheter och friheter, inklusive socialt skydd, folkhälsa och humanitära skäl. Dessa begränsningar bör överensstämma med kraven i stadgan och den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna.

(74) Personuppgiftsansvariga bör åläggas ansvaret för all behandling av personuppgifter som de utför eller som utförs på deras vägnar. Personuppgiftsansvariga bör särskilt vara skyldiga att vidta lämpliga och effektiva åtgärder och kunna visa att behandlingen är förenlig med denna förordning, även vad gäller åtgärdernas effektivitet. Man bör inom dessa åtgärder beakta behandlingens art, omfattning, sammanhang och ändamål samt risken för fysiska personers rättigheter och friheter.

(75) Risken för fysiska personers rättigheter och friheter, av varierande sannolikhetsgrad och allvar, kan uppkomma till följd av personuppgiftsbehandling som skulle kunna medföra fysiska, materiella eller immateriella skador, i synnerhet om behandlingen kan leda till diskriminering, identitetsstöld eller bedrägeri, ekonomisk förlust, skadat anseende, förlust av konfidentialitet när det gäller personuppgifter som omfattas av tystnadsplikt, obehörigt hävande av pseudonymisering eller annan betydande ekonomisk eller social nackdel, om registrerade kan berövas sina rättigheter och friheter eller hindras att utöva kontroll över sina personuppgifter, om personuppgifter behandlas som avslöjar ras eller etniskt ursprung, politiska åsikter, religion eller övertygelse eller medlemskap i fackförening, om genetiska uppgifter, uppgifter om hälsa eller sexualliv eller fällande domar i brottmål samt överträdelser eller därmed sammanhängande säkerhetsåtgärder behandlas, om personliga aspekter bedöms, framför allt analyser eller förutsägelser beträffande sådant som rör arbetsprestationer, ekonomisk ställning, hälsa, personliga preferenser eller intressen, tillförlitlighet eller beteende, vistelseort eller förflyttningar, i syfte att skapa eller använda personliga profiler, om det sker behandling av personuppgifter rörande sårbara fysiska personer, framför allt barn, eller om behandlingen inbegriper ett stort antal personuppgifter och gäller ett stort antal registrerade.

(76) Hur sannolik och allvarlig risken för den registrerades rättigheter och friheter är bör fastställas utifrån behandlingens art, omfattning, sammanhang och ändamål. Risken bör utvärderas på grundval av en objektiv bedömning, genom vilken det fastställs huruvida uppgiftsbehandlingen inbegriper en risk eller en hög risk.

(77) Vägledning för den personuppgiftsansvariges eller personuppgiftsbiträdets genomförande av lämpliga åtgärder och för påvisande av att behandlingen är förenlig med denna förordning, särskilt när det gäller att kartlägga den risk som är förknippad med behandlingen och bedöma dess ursprung, art, sannolikhetsgrad och allvar samt fastställa bästa praxis för att minska risken, kan framför allt ges genom godkända uppförandekoder, godkänd certifiering, riktlinjer från styrelsen eller genom anvisningar från ett dataskyddsombud. Styrelsen kan också utfärda riktlinjer för uppgiftsbehandling som inte bedöms medföra någon hög risk för fysiska personers rättigheter och friheter samt ange vilka åtgärder som i sådana fall kan vara tillräckliga för att bemöta en sådan risk.

(78) Skyddet av fysiska personers rättigheter och friheter i samband med behandling av personuppgifter förutsätter att lämpliga tekniska och organisatoriska åtgärder vidtas, så att kraven i denna förordning uppfylls. För att kunna visa att denna förordning följs bör den personuppgiftsansvarige anta interna strategier och vidta åtgärder, särskilt för att uppfylla principerna om inbyggt dataskydd och dataskydd som standard. Sådana åtgärder kan bland annat bestå av att uppgiftsbehandlingen minimeras, att personuppgifter snarast möjligt pseudonymiseras, att öppenhet om personuppgifternas syfte och behandling iakttas, att den registrerade får möjlighet att övervaka uppgiftsbehandlingen och att den personuppgiftsansvarige får möjlighet att skapa och förbättra säkerhetsanordningar. Vid utveckling, utformning, urval och användning av applikationer, tjänster och produkter som är baserade på behandling av personuppgifter eller behandlar personuppgifter för att uppfylla sitt syfte bör producenterna av dessa produkter, tjänster och applikationer uppmanas att beakta rätten till dataskydd när sådana produkter, tjänster och applikationer utvecklas och utformas och att, med tillbörlig hänsyn till den tekniska utvecklingen, säkerställa att personuppgiftsansvariga och personuppgiftsbiträden kan fullgöra sina skyldigheter avseende dataskydd. Principerna om inbyggt dataskydd och dataskydd som standard bör också beaktas vid offentliga upphandlingar.

(79) Skyddet av de registrerades rättigheter och friheter samt de personuppgiftsansvarigas och personuppgiftsbiträdenas ansvar, även i förhållande till tillsynsmyndigheternas övervakning och åtgärder, kräver ett tydligt fastställande av vem som bär ansvaret enligt denna förordning, bl.a. när personuppgiftsansvariga gemensamt fastställer ändamål och medel för en behandling tillsammans med andra personuppgiftsansvariga eller när en behandling utförs på en personuppgiftsansvarigs vägnar.

(80) När personuppgiftsansvariga eller personuppgiftsbiträden som inte är etablerade inom unionen behandlar personuppgifter om registrerade som befinner sig inom unionen och det bakomliggande syftet med uppgiftsbehandlingen är att erbjuda de registrerade personerna i unionen varor eller tjänster, oberoende av om de registrerade personerna måste betala för dem, eller att övervaka deras beteende i den mån beteendet äger rum i unionen, bör de personuppgiftsansvariga eller personuppgiftsbiträdena utnämna en företrädare, såvida inte behandlingen endast är tillfällig, inte omfattar behandling i stor omfattning av särskilda kategorier av personuppgifter eller behandling av personuppgifter om fällande domar i brottmål samt överträdelser och det är

osannolikt att den inbegriper en risk för fysiska personers rättigheter och friheter, med beaktande av behandlingens art, sammanhang, omfattning och ändamål eller om den personuppgiftsansvarige är en myndighet eller ett organ. Företrädaren bör agera på den personuppgiftsansvariges eller på personuppgiftsbiträdets vägnar och kan kontaktas av samtliga tillsynsmyndigheter. Företrädaren bör uttryckligen utses genom en skriftlig fullmakt från den personuppgiftsansvarige eller från personuppgiftsbiträdet att agera på dennes vägnar med avseende på dennes skyldigheter enligt denna förordning. Utnämningen av företrädaren inverkar inte på den personuppgiftsansvariges eller på personuppgiftsbiträdets ansvar enligt denna förordning. Företrädaren bör utföra sina uppgifter i enlighet med erhållen fullmakt från den personuppgiftsansvarige eller från personuppgiftsbiträdet, vilket inbegriper samarbete med de behöriga tillsynsmyndigheterna i fråga om alla åtgärder som vidtas för att sörja för efterlevnad av denna förordning. Den utsedda företrädaren bör underkastas verkställighetsförfaranden i händelse den personuppgiftsansvarige eller personuppgiftsbiträdet inte uppfyller sina skyldigheter.

(81) För att se till att kraven i denna förordning uppfylls vad gäller behandling som av ett personuppgiftsbiträde ska utföras på en personuppgiftsansvarigs vägnar ska den personuppgiftsansvarige, när denne anförtror behandling åt ett personuppgiftsbiträde, endast använda personuppgiftsbiträden som ger tillräckliga garantier, i synnerhet i fråga om sakkunskap, tillförlitlighet och resurser, för att genomföra tekniska och organisatoriska åtgärder som uppfyller kraven i denna förordning, bl.a. vad gäller säkerhet i samband med behandlingen av uppgifter. Personuppgiftsbiträdets anslutning till en godkänd uppförandekod eller en godkänd certifieringsmekanism kan användas som ett sätt att påvisa att den personuppgiftsansvarige fullgör sina skyldigheter. När uppgifter behandlas av ett personuppgiftsbiträde, bör hanteringen regleras genom ett avtal eller en annan rättsakt enligt unionsrätten eller medlemsstaternas nationella rätt mellan personuppgiftsbiträdet och den personuppgiftsansvarige, där föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade anges, med beaktande av personuppgiftsbiträdets specifika arbets- och ansvarsuppgifter inom ramen för den behandling som ska utföras och risken med avseende på den registrerades rättigheter och friheter. Den personuppgiftsansvarige och personuppgiftsbiträdet får välja att använda sig av ett enskilt avtal eller standardavtalsklausuler som antingen antas direkt av kommissionen eller av en tillsynsmyndighet i enlighet med mekanismen för enhetlighet och därefter antas av kommissionen. Efter det att behandlingen på den personuppgiftsansvariges vägnar har avslutats, bör personuppgiftsbiträdet återlämna eller radera personuppgifterna, beroende på vad den personuppgiftsansvarige väljer, såvida inte lagring av personuppgifterna krävs enligt den unionsrätt eller medlemsstaternas nationella rätt som personuppgiftsbiträdet omfattas av.

(82) För att påvisa att denna förordning följs bör de personuppgiftsansvariga eller personuppgiftsbiträdena föra register över behandling som sker under deras ansvar. Alla personuppgiftsansvariga och personuppgiftsbiträden bör vara skyldiga att samarbeta med tillsynsmyndigheten och på dennas begäran göra detta register tillgängligt, så att det kan tjäna som grund för övervakningen av behandlingen.

(83) För att upprätthålla säkerheten och förhindra behandling som bryter mot denna förordning bör personuppgiftsansvariga eller personuppgiftsbiträden utvärdera riskerna med behandlingen och vidta åtgärder, såsom kryptering, för att minska dem. Åtgärderna bör säkerställa en lämplig säkerhetsnivå, inbegripet konfidentialitet, med beaktande av den senaste utvecklingen och genomförandekostnader i förhållande till riskerna och vilken typ av personuppgifter som ska skyddas. Vid bedömningen av datasäkerhetsrisken bör man även beakta de risker som personuppgiftsbehandling medför, såsom förstöring, förlust eller ändringar genom olyckshändelse eller otillåtna handlingar eller obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats, framför allt när denna kan medföra fysisk, materiell eller immateriell skada.

(84) I syfte att sörja för bättre efterlevnad av denna förordning när behandlingen sannolikt kan innebära en hög risk för fysiska personers rättigheter och friheter, bör den personuppgiftsansvarige vara ansvarig för att en konsekvensbedömning utförs avseende datasskydd för att bedöma framför allt riskens ursprung, art, särdrag och allvar. Resultatet av denna bedömning bör beaktas vid fastställandet av de lämpliga åtgärder som ska vidtas för att visa att behandlingen av personuppgifter är förenlig med denna förordning. I de fall en konsekvensbedömning avseende dataskydd ger vid handen att uppgiftsbehandlingen medför en hög risk, som den personuppgiftsansvarige inte kan begränsa genom lämpliga åtgärder med avseende på tillgänglig teknik och genomförandekostnader, bör ett samråd med tillsynsmyndigheten ske före behandlingen.

(85) En personuppgiftsincident som inte snabbt åtgärdas på lämpligt sätt kan för fysiska personer leda till fysisk, materiell eller immateriell skada, såsom förlust av kontrollen över de egna personuppgifterna eller till begränsning av deras rättigheter, diskriminering, identitetsstöld eller bedrägeri, ekonomisk förlust, obehörigt hävande av pseudonymisering, skadat anseende, förlust av konfidentialitet när det gäller personuppgifter som omfattas av tystnadsplikt, eller till annan ekonomisk eller social nackdel för den berörda fysiska personen. Så

snart en personuppgiftsansvarig blir medveten om att en personuppgiftsincident har inträffat, bör den personuppgiftsansvarige därför anmäla personuppgiftsincidenten till tillsynsmyndigheten utan onödigt dröjsmål och, om så är möjligt, inom 72 timmar efter att ha blivit medveten om denna, om inte den personuppgiftsansvarige, i enlighet med ansvarsprincipen, kan påvisa att det är osannolikt att personuppgiftsincidenten kommer att medföra en risk för fysiska personers rättigheter och friheter. Om en sådan anmälan inte kan ske inom 72 timmar, bör skälen till fördröjningen åtfölja anmälan och information får lämnas i omgångar utan otillbörligt vidare dröjsmål.

(86) Den personuppgiftsansvarige bör utan onödigt dröjsmål underrätta den registrerade om en personuppgiftsincident, om personuppgiftsincidenten sannolikt kommer att medföra en hög risk för den fysiska personens rättigheter och friheter, så att denne kan vidta nödvändiga försiktighetsåtgärder. Denna underrättelse bör beskriva personuppgiftsincidentens art samt innehålla rekommendationer för den berörda fysiska personen om hur de potentiella negativa effekterna kan mildras. De registrerade bör underrättas så snart detta rimligtvis är möjligt, i nära samarbete med tillsynsmyndigheten och i enlighet med den vägledning som lämnats av den eller andra relevanta myndigheter, exempelvis brottsbekämpande myndigheter. Till exempel kräver behovet av att mildra en omedelbar skaderisk att de registrerade underrättas omedelbart, medan behovet av att vidta lämpliga åtgärder vid fortlöpande eller likartade personuppgiftsincidenter däremot kan motivera längre tid för underrättelsen.

(87) Det bör undersökas huruvida alla lämpliga tekniska skyddsåtgärder och alla lämpliga organisatoriska åtgärder har vidtagits för att omedelbart fastställa om en personuppgiftsincident har ägt rum och skyndsamt informera tillsynsmyndigheten och den registrerade. Att en anmälan gjordes utan onödigt dröjsmål bör fastställas med hänsyn tagen bl.a. till personuppgiftsincidentens art och svårighetsgrad och dess följder och negativa effekter för den registrerade. En sådan anmälan kan leda till ett ingripande från tillsynsmyndighetens sida i enlighet med dess uppgifter och befogenheter enligt denna förordning.

(88) När ingående regler fastställs för format och förfaranden för anmälan av personuppgiftsincidenter, bör vederbörlig hänsyn tas till omständigheterna kring incidenten, däribland om personuppgifterna var skyddade av lämpliga tekniska skyddsåtgärder, som betydligt begränsar sannolikheten för identitetsbedrägeri eller andra former av missbruk. Dessutom bör sådana regler och förfaranden beakta brottsbekämpande myndigheters berättigade intressen, där en för tidig redovisning kan riskera att i onödan hämma utredning av omständigheterna kring en personuppgiftsincident.

(89) Direktiv 95/46/EG föreskrev en allmän skyldighet att anmäla behandling av personuppgifter till tillsynsmyndigheterna. Denna skyldighet medförde administrativa och ekonomiska bördor, men förbättrade inte alltid personuppgiftsskyddet. Sådana övergripande och allmänna anmälningsskyldigheter bör därför avskaffas och ersättas av effektiva förfaranden och mekanismer som i stället inriktas på de typer av behandlingar som sannolikt innebär en hög risk för fysiska personers rättigheter och friheter, i kraft av deras art, omfattning, sammanhang och ändamål. Dessa behandlingar kan vara sådana som särskilt inbegriper användning av ny teknik eller är av en ny typ, för vilken konsekvensbedömning avseende uppgiftsskydd inte tidigare har genomförts av den personuppgiftsansvarige, eller som blir nödvändiga på grund av den tid som har förflutit sedan den ursprungliga behandlingen.

(90) I sådana fall bör den personuppgiftsansvarige före behandlingen, med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt upphovet till risken, göra en konsekvensbedömning avseende dataskydd i syfte att bedöma den höga riskens specifika sannolikhetsgrad och allvar samt dess ursprung. Konsekvensbedömningen bör främst innefatta de planerade åtgärder, skyddsåtgärder och mekanismer som ska minska denna risk, säkerställa personuppgiftskyddet och visa att denna förordning efterlevs.

(91) Detta bör särskilt vara tillämpligt på storskalig uppgiftsbehandling med syftet att behandla betydande mängder personuppgifter på regional, nationell eller övernationell nivå, vilket skulle kunna påverka ett stort antal registrerade och sannolikt kommer att innebära en hög risk, exempelvis till följd av uppgifternas känsliga natur, där i enlighet med den uppnådda nivån av teknisk kunskap en ny teknik används storskaligt, samt på annan behandling som innebär en hög risk för registrerades rättigheter och friheter, framför allt när denna behandling gör det svårare för de registrerade att utöva sina rättigheter. En konsekvensbedömning avseende dataskydd bör

också göras, där personuppgifter behandlas i syfte att fatta beslut om specifika fysiska personer efter en systematisk och omfattande bedömning av fysiska personers personliga aspekter på grundval av profilering av dessa uppgifter eller efter behandling av särskilda kategorier av personuppgifter, biometriska uppgifter eller uppgifter om fällande domar i brottmål samt överträdelser eller därmed sammanhängande säkerhetsåtgärder. Likaså krävs en konsekvensbedömning avseende dataskydd för övervakning av allmän plats i stor omfattning, särskilt vid användning av optisk-elektroniska anordningar, eller för all annan behandling där den behöriga tillsynsmyndigheten anser att behandlingen sannolikt kommer att innebära en hög risk för de registrerades rättigheter och friheter, framför allt på grund av att den hindrar de registrerade från att utöva en rättighet eller använda en tjänst eller ett avtal eller på grund av att den systematiskt genomförs i stor omfattning. Behandling av personuppgifter bör inte anses vara storskalig, om det är fråga om personuppgifter från patienter eller klienter som behandlas av enskilda läkare, andra yrkesverksamma på hälsoområdet eller juridiska ombud. I dessa fall bör en konsekvensbedömning avseende dataskydd inte vara obligatorisk.

(92) Ibland kan det vara förnuftigt och ekonomiskt att en konsekvensbedömning avseende dataskydd inriktar sig på ett vidare område än ett enda projekt, exempelvis när myndigheter eller organ avser att skapa en gemensam tillämpnings- eller behandlingsplattform eller när flera personuppgiftsansvariga planerar att införa en gemensam tillämpnings- eller behandlingsmiljö för en hel bransch eller ett helt segment eller för en allmänt utnyttjad horisontell verksamhet.

(93) Medlemsstaterna kan anse det nödvändigt att genomföra en sådan bedömning före behandlingen i samband med antagandet av medlemsstaters nationella rätt som ligger till grund för utförandet av myndighetens eller det offentliga organets uppgifter och reglerar den aktuella specifika behandlingsåtgärden eller serien av åtgärder.

(94) Om det av en konsekvensbedömning avseende dataskydd framgår att behandlingen utan skyddsåtgärder, säkerhetsåtgärder och mekanismer för att minska risken kommer att innebära en hög risk för fysiska personers rättigheter och friheter, och den personuppgiftsansvarige anser att risken inte kan begränsas genom åtgärder som är rimliga med avseende på tillgänglig teknik och genomförandekostnader, bör samråd hållas med tillsynsmyndigheten innan behandlingen inleds. En sådan hög risk kommer sannolikt att orsakas av vissa typer av behandling samt av en viss omfattning och frekvens för behandlingen, vilket även kan leda till skador för eller kränkningar av fysiska personers rättigheter och friheter. Tillsynsmyndigheten bör inom en fastställd tid svara på en begäran om samråd. Ett uteblivet svar från tillsynsmyndigheten inom denna tid bör dock inte hindra ett eventuellt ingripande från tillsynsmyndighetens sida i enlighet med dess uppgifter och befogenheter enligt denna förordning, inbegripet befogenheten att förbjuda behandling. Som en del av denna samrådsprocess får resultatet av en konsekvensbedömning avseende dataskydd som utförs med avseende på behandlingen i fråga överlämnas till tillsynsmyndigheten, framför allt de åtgärder som planeras för att minska risken för fysiska personers rättigheter och friheter.

(95) Personuppgiftsbiträdet bör vid behov och på begäran bistå den personuppgiftsansvarige med fullgörande av de skyldigheter som härrör från utförandet av konsekvensbedömningar avseende dataskydd och förhandssamråd med tillsynsmyndigheten.

(96) Ett samråd med tillsynsmyndigheten bör även ske som ett led i det förberedande arbetet med en lagstiftningsåtgärd som stadgar om behandling av personuppgifter i syfte att säkerställa att den avsedda behandlingen överensstämmer med denna förordning och framför allt för att minska den risk den medför för den registrerade.

(97) När en behandling utförs av en myndighet, med undantag av domstolar eller oberoende rättsliga myndigheter som en del av deras dömande verksamhet, eller när en behandling utförs i den privata sektorn av en personuppgiftsansvarig vars kärnverksamhet består av behandlingsverksamhet som kräver regelbunden och systematisk övervakning av de registrerade i stor omfattning, eller när den personuppgiftsansvariges eller personuppgiftsbiträdets kärnverksamhet består av behandling i stor omfattning av särskilda kategorier av personuppgifter och uppgifter som rör fällande domar i brottmål och överträdelser, bör en person med sakkunskap i fråga om dataskyddslagstiftning och -förfaranden bistå den personuppgiftsansvarige eller personuppgiftsbiträdet för att övervaka den interna efterlevnaden av denna förordning. I den privata sektorn avser personuppgiftsansvarigas kärnverksamhet deras primära verksamhet och inte behandling av personuppgifter som kompletterande verksamhet. Den nödvändiga nivån på sakkunskapen bör fastställas särskilt i enlighet med den uppgiftsbehandling

som utförs och det skydd som krävs för de personuppgifter som behandlas av den personuppgiftsansvarige eller personuppgiftsbiträdet. Denna typ av dataskyddsombud bör, oavsett om de är anställda av den personuppgiftsansvarige eller ej, kunna fullgöra sitt uppdrag och utföra sina uppgifter på ett oberoende sätt.

(98) Sammanslutningar eller andra organ som företräder kategorier av personuppgiftsansvariga eller personuppgiftsbiträden bör uppmuntras att utarbeta uppförandekoder inom gränserna för denna förordning, så att tillämpningen av denna förordning effektiviseras, med beaktande av särdragen hos den behandling som sker inom vissa sektorer och de särskilda behov som finns inom mikroföretag samt inom små och medelstora företag. I synnerhet skulle man genom sådana uppförandekoder kunna anpassa personuppgiftsansvarigas och personuppgiftsbiträdens skyldigheter, med beaktande av den risk som behandlingen sannolikt innebär för fysiska personers rättigheter och friheter.

(99) Vid utformningen av en uppförandekod eller vid ändring eller utvidgning av en befintlig sådan kod bör sammanslutningar och andra organ som företräder kategorier av personuppgiftsansvariga eller personuppgiftsbiträden samråda med berörda intressenter, i möjligaste mån inbegripet registrerade, och beakta de inlagor som mottas och de åsikter som framförs som svar på samråden.

(100) För att förbättra öppenheten och efterlevnaden av denna förordning bör införandet av certifieringsmekanismer och dataskyddsförsegling och dataskyddsmärkning uppmuntras, så att registrerade snabbt kan bedöma nivån på relevanta produkters och tjänsters dataskydd.

(101) Flöden av personuppgifter till och från länder utanför unionen och till och från internationella organisationer är nödvändiga för utvecklingen av internationell handel och internationellt samarbete. Ökningen av dessa flöden har medfört nya utmaningar och nya farhågor när det gäller skyddet av personuppgifter. Det är viktigt att den skyddsnivå som fysiska personer säkerställs inom unionen genom denna förordning inte undergrävs när personuppgifter överförs från unionen till personuppgiftsansvariga, personuppgiftsbiträden eller andra mottagare i tredjeland eller till internationella organisationer, vilket inbegriper vidarebefordran av personuppgifter från tredjelandet eller den internationella organisationen till personuppgiftsansvariga, personuppgiftsbiträden i samma eller ett annat tredjeland eller en annan internationell organisation. Överföringar till tredjeländer och internationella organisationer får under alla omständigheter endast utföras i full överensstämmelse med denna förordning. En överföring kan endast ske, om de villkor som fastställs i bestämmelserna i denna förordning om överföring av personuppgifter till tredjeländer eller internationella organisationer har uppfyllts av den personuppgiftsansvarige eller personuppgiftsbiträdet, med förbehåll för de övriga bestämmelserna i denna förordning.

(102) Denna förordning påverkar inte internationella avtal mellan unionen och tredjeländer som reglerar överföring av personuppgifter, däribland lämpliga skyddsåtgärder för de registrerade. Medlemsstaterna får ingå internationella avtal som innefattar överföring av personuppgifter till tredjeländer eller internationella organisationer i den mån sådana avtal inte påverkar denna förordning eller andra bestämmelser i unionsrätten och innehåller en skälig nivå av skydd för de registrerades grundläggande rättigheter.

(103) Kommissionen kan med verkan för hela unionen fastställa att ett tredjeland, ett territorium eller en specificerad sektor i ett tredjeland eller en internationell organisation erbjuder en adekvat dataskyddsnivå och på så sätt skapa rättslig säkerhet och enhetlighet i hela unionen vad gäller tredjelandet eller den internationella organisationen som anses tillhandahålla en sådan skyddsnivå. I dessa fall får överföringar av personuppgifter till det tredjelandet eller den internationella organisationen ske utan ytterligare tillstånd. Kommissionen kan också, efter att ha underrättat tredjelandet eller den internationella organisationen och lämnat en fullständig motivering, besluta att ett sådant beslut ska återkallas.

(104) I enlighet med de grundläggande värderingar som unionen bygger på, bl.a. skyddet av mänskliga rättigheter, bör kommissionen i sin bedömning av tredjelandet eller ett territorium eller en specificerad sektor i ett tredjeland beakta hur ett visst tredjeland respekterar rättsstatsprincipen, tillgången till rättslig prövning samt internationella människorättsnormer och -standarder samt landets allmänna lagstiftning och sektorslagstiftning, inklusive lagstiftning om allmän säkerhet, försvar och nationell säkerhet samt allmän ordning och straffrätt. Vid antagandet av ett beslut om adekvat skyddsnivå avseende ett territorium eller en specificerad sektor i ett tredjeland bör hänsyn tas till tydliga och objektiva kriterier, t.ex. specifik behandling och tillämpningsområdet för tillämpliga rättsliga standarder och gällande lagstiftning i tredjelandet. Tredjelandet bör erbjuda garantier som säkerställer en

tillfredsställande skyddsnivå som i huvudsak motsvarar den som säkerställs i unionen, i synnerhet när personuppgifter behandlas inom en eller flera specifika sektorer. Tredjelandet bör framför allt säkerställa en effektiv oberoende dataskyddsövervakning och sörja för samarbetsmekanismer med medlemsstaternas dataskyddsmyndigheter, och de registrerade bör tillförsäkras effektiva och lagstadgade rättigheter samt effektiv administrativ och rättslig prövning.

(105) Utöver de internationella åtaganden som tredjelandet eller den internationella organisationen har gjort bör kommissionen beakta de skyldigheter som följer av tredjelandets eller den internationella organisationens deltagande i multilaterala eller regionala system, särskilt rörande skydd av personuppgifter och genomförandet av dessa skyldigheter. Framför allt bör tredjelandets anslutning till Europarådets konvention av den 28 januari 1981 om skydd för enskilda vid automatisk behandling av personuppgifter och dess tilläggsprotokoll beaktas. Kommissionen bör samråda med styrelsen vid bedömningen av skyddsnivån i tredjeländer eller internationella organisationer.

(106) Kommissionen bör övervaka hur beslut om skyddsnivå i ett tredjeland, ett territorium eller en specificerad sektor i ett tredjeland eller en internationell organisation fungerar, och övervaka hur beslut som antas på grundval av artikel 25.6 eller 26.4 i direktiv 95/46/EG fungerar. Kommissionen bör i sina beslut om adekvat skyddsnivå föreskriva en mekanism för periodisk översyn av hur de fungerar. Denna periodiska översyn bör genomföras i samråd med det berörda tredjelandet eller den berörda internationella organisationen, med beaktande av all relevant utveckling i tredjelandet eller den internationella organisationen. Vid övervakningen och genomförandet av den periodiska översynen bör kommissionen ta hänsyn till synpunkter och resultat från Europaparlamentet och rådet samt andra relevanta organ och källor. Kommissionen bör inom rimlig tid utvärdera hur de sistnämnda besluten fungerar och rapportera alla relevanta resultat till den kommitté, i den mening som avses i Europaparlamentets och rådets förordning (EU) nr 182/2011 ([1]), som inrättats enligt denna förordning och till Europaparlamentet och rådet.

(107) Kommissionen kan konstatera att ett tredjeland, ett territorium eller en viss specificerad sektor i ett tredjeland eller en internationell organisation inte längre säkerställer en adekvat dataskyddsnivå. Överföring av personuppgifter till detta tredjeland eller till denna internationella organisation bör då förbjudas, såvida inte kraven i denna förordning avseende överföring med stöd av lämpliga skyddsåtgärder, inbegripet bindande företagsbestämmelser och undantag för särskilda situationer, är uppfyllda. I så fall bör det finnas möjlighet till samråd mellan kommissionen och dessa tredjeländer eller internationella organisationer. Kommissionen bör i god tid informera tredjelandet eller den internationella organisationen om skälen och inleda samråd med tredjelandet eller organisationen för att avhjälpa situationen.

(108) Saknas beslut om adekvat skyddsnivå bör den personuppgiftsansvarige eller personuppgiftsbiträdet vidta åtgärder för att kompensera för det bristande dataskyddet i ett tredjeland med hjälp av lämpliga skyddsåtgärder för den registrerade. Sådana lämpliga skyddsåtgärder kan bestå i tillämpning av bindande företagsbestämmelser, standardbestämmelser om dataskydd som antagits av kommissionen, standardbestämmelser om dataskydd som antagits av en tillsynsmyndighet eller avtalsbestämmelser som godkänts av en tillsynsmyndighet. Dessa skyddsåtgärder bör säkerställa iakttagande av de krav i fråga om dataskydd och registrerades rättigheter som är lämpliga för behandling inom unionen, inbegripet huruvida bindande rättigheter för de registrerade och effektiva rättsmedel är tillgängliga, inbegripet en faktisk rätt att föra talan på administrativ väg eller inför domstol och att kräva kompensation i unionen eller i ett tredjeland. De bör särskilt gälla överensstämmelse med allmänna principer för behandling av personuppgifter samt principerna om inbyggt dataskydd och dataskydd som standard. Överföring av uppgifter kan också utföras av offentliga myndigheter eller organ till offentliga myndigheter eller organ i tredjeländer eller internationella organisationer med motsvarande skyldigheter eller uppgifter, inbegripet på grundval av bestämmelser som ska införas i administrativa överenskommelser, t.ex. samförståndsavtal, som föreskriver verkställbara och faktiska rättigheter för de registrerade. Tillstånd från den behöriga tillsynsmyndigheten bör erhållas när skyddsåtgärder föreskrivs i icke rättsligt bindande administrativa arrangemang.

(109) Personuppgiftsansvarigas eller personuppgiftsbiträdens möjlighet att använda standardiserade dataskyddsbestämmelser som antagits av kommissionen eller av en tillsynsmyndighet bör inte hindra att de infogar

([1]) Europaparlamentets och rådets förordning (EU) nr 182/2011 av den 16 februari 2011 om fastställande av allmänna regler och principer för medlemsstaternas kontroll av kommissionens utövande av sina genomförandebefogenheter (EUT L 55, 28.2.2011, s. 13).

standardiserade dataskyddsbestämmelser i ett vidare avtal, såsom ett avtal mellan personuppgiftsbiträdet och ett annat personuppgiftsbiträde, eller lägger till andra bestämmelser eller ytterligare skyddsåtgärder, under förutsättning att de inte direkt eller indirekt står i strid med standardavtalsklausuler som antagits av kommissionen eller av en tillsynsmyndighet eller påverkar de registrerades grundläggande rättigheter eller friheter. Personuppgiftsansvariga och personuppgiftsbiträden bör uppmuntras att tillhandahålla ytterligare skyddsåtgärder via avtalsmässiga åtaganden som kompletterar de standardiserade skyddsbestämmelserna.

(110) En koncern eller en grupp av företag som deltar i en gemensam ekonomisk verksamhet bör kunna använda sig av godkända bindande företagsbestämmelser för sina internationella överföringar från unionen till organisationer inom samma koncern eller grupp av företag som deltar i en gemensam ekonomisk verksamhet, under förutsättning att företagsbestämmelserna inbegriper alla nödvändiga principer och bindande rättigheter som säkerställer lämpliga skyddsåtgärder för överföringar eller kategorier av överföringar av personuppgifter.

(111) Det bör införas bestämmelser som ger möjlighet att under vissa omständigheter göra överföringar, om den registrerade har lämnat sitt uttryckliga samtycke, när överföringen är tillfällig och nödvändig med hänsyn till ett avtal eller ett rättsligt anspråk, oavsett om detta sker inom ett rättsligt förfarande eller i ett administrativt eller utomrättsligt förfarande, inbegripet förfaranden inför tillsynsorgan. Det bör också införas bestämmelser som ger möjlighet till överföringar om viktiga allmänintressen fastställda genom unionsrätten eller medlemsstaternas nationella rätt så kräver eller när överföringen görs från ett register som inrättats genom lag och är avsett att konsulteras av allmänheten eller av personer med ett berättigat intresse. I sistnämnda fall bör en sådan överföring inte omfatta alla personuppgifter eller hela kategorier av uppgifter i registret, och överföringen bör endast göras när registret är avsett att vara tillgängligt för personer med ett berättigat intresse, på begäran av dessa personer eller om de själva är mottagarna, med full hänsyn till de registrerades intressen och grundläggande rättigheter.

(112) Dessa undantag bör främst vara tillämpliga på uppgiftsöverföringar som krävs och är nödvändiga med hänsyn till viktiga allmänintressen, exempelvis vid internationella utbyten av uppgifter mellan konkurrensmyndigheter, skatte- eller tullmyndigheter, finanstillsynsmyndigheter, socialförsäkringsmyndigheter eller hälsovårdsmyndigheter, till exempel vid kontaktspårning för smittsamma sjukdomar eller för att minska och/eller undanröja dopning inom idrott. En överföring av personuppgifter bör också betraktas som laglig, om den är nödvändig för att skydda ett intresse som är väsentligt för den registrerades eller en annan persons vitala intressen, inklusive dennes fysiska integritet och liv, om den registrerade är oförmögen att ge sitt samtycke. Saknas beslut om adekvat skyddsnivå får unionsrätten eller medlemsstaternas nationella rätt med hänsyn till viktiga allmänintressen uttryckligen fastställa gränser för överföringen av särskilda kategorier av uppgifter till ett tredjeland eller en internationell organisation. Medlemsstaterna bör underrätta kommissionen om sådana bestämmelser. Varje överföring till en internationell humanitär organisation av personuppgifter rörande en registrerad som är fysiskt eller rättsligt förhindrad att ge sitt samtycke, i syfte att utföra en uppgift inom ramen för Genèvekonventionerna eller vara förenlig med internationell humanitär rätt, vilken är tillämplig vid väpnade konflikter, skulle kunna anses vara nödvändig för ett betydande allmänintresse eller för att den är av vitalt intresse för den registrerade.

(113) Överföringar som kan anses vara icke återkommande och endast gäller ett begränsat antal registrerade kan också vara möjliga när personuppgiftsansvarigas tvingande berättigade intressen motiverar detta, om inte den registrerades intressen eller rättigheter och friheter väger tyngre än dessa intressen, och den personuppgiftsansvarige har bedömt alla omständigheter kring uppgiftsöverföringen. Den personuppgiftsansvarige bör ta särskild hänsyn till personuppgifternas art, den eller de avsedda behandlingarnas ändamål och varaktighet samt situationen i ursprungslandet, tredjelandet och det slutliga bestämmelselandet och bör tillhandahålla lämpliga åtgärder för att skydda fysiska personers grundläggande rättigheter och friheter vid behandlingen av deras personuppgifter. Sådana överföringar bör endast vara möjliga i vissa fall där inget av de andra skälen till överföring är tillämpligt. För vetenskapliga eller historiska forskningsändamål eller statistiska ändamål bör hänsyn tas till samhällets legitima förväntningar i fråga om ökad kunskap. Den personuppgiftsansvarige bör informera tillsynsmyndigheten och den registrerade om överföringen.

(114) Om kommissionen inte har fattat beslut om adekvat dataskyddsnivå i ett tredjeland, bör den personuppgiftsansvarige eller personuppgiftsbiträdet i alla fall använda sig av lösningar som ger de registrerade verkställbara och effektiva rättigheter vad gäller behandlingen av deras personuppgifter inom unionen när dessa uppgifter väl har överförts, så att de fortsatt kan utöva sina grundläggande rättigheter och att skyddsåtgärder fortsatt gäller i förhållande till dem.

(115) Vissa tredjeländer antar lagar och andra författningar som syftar till att direkt reglera behandling som genomförs av fysiska och juridiska personer under medlemsstaternas jurisdiktion. Detta kan inkludera rättsliga avgöranden eller beslut av administrativa myndigheter i tredjeländer med krav på att personuppgiftsansvariga eller personuppgiftsbiträden överför eller överlämnar personuppgifter, vilka inte grundar sig på något gällande internationellt avtal, såsom ett fördrag om ömsesidig rättshjälp, mellan det begärande tredjelandet och unionen eller en medlemsstat. Extraterritoriell tillämpning av dessa lagar och andra författningar kan strida mot internationell rätt och inverka menligt på det skydd av fysiska personer som säkerställs inom unionen genom denna förordning. Överföringar bör endast tillåtas om villkoren i denna förordning för en överföring till tredjeländer är uppfyllda. Detta kan vara fallet bl.a. när utlämnande är nödvändigt på grund av ett viktigt allmänintresse som erkänns i unionsrätten eller i medlemsstaternas nationella rätt som den personuppgiftsansvarige omfattas av.

(116) När personuppgifter förs över gränser utanför unionen kan detta öka risken för att fysiska personer inte kan utöva sina dataskyddsrättigheter, i synnerhet för att skydda sig från otillåten användning eller otillåtet utlämnande av denna information. Samtidigt kan tillsynsmyndigheter finna att de inte är i stånd att handlägga klagomål eller göra utredningar som gäller verksamheter utanför gränserna för deras land. Deras strävan att arbeta tillsammans över gränserna kan också hindras av otillräckliga preventiva eller korrigerande befogenheter, oenhetliga rättsliga regelverk och praktiska hinder, som exempelvis bristande resurser. Närmare samarbete mellan dataskyddstillsynsmyndigheter bör därför främjas för att hjälpa dem att utbyta information och utföra utredningar med sina internationella motparter. I syfte att bygga upp internationella samarbetsmekanismer för att underlätta och tillhandahålla ömsesidig internationell hjälp med att kontrollera efterlevnaden av lagstiftningen till skydd för personuppgifter, bör kommissionen och tillsynsmyndigheterna utbyta information och samarbeta, inom verksamhet som rör utövandet av deras befogenheter, med behöriga myndigheter i tredjeländer, på grundval av ömsesidighet och i överensstämmelse med denna förordning.

(117) Ett väsentligt inslag i skyddet av fysiska personer vid behandlingen av personuppgifter är att medlemsstaterna inrättar tillsynsmyndigheter med behörighet att utföra sina uppgifter och utöva sina befogenheter under fullständigt oberoende. Medlemsstaterna bör kunna inrätta fler än en tillsynsmyndighet om det behövs för att ta hänsyn till den egna konstitutionella, organisatoriska och administrativa strukturen.

(118) Tillsynsmyndigheternas oberoende bör dock inte innebära att deras utgifter inte kan underkastas kontroll- eller övervakningsmekanismer eller bli föremål för domstolsprövning.

(119) Om en medlemsstat inrättar flera tillsynsmyndigheter, bör den genom lagstiftning säkerställa att dessa tillsynsmyndigheter effektivt deltar i mekanismen för enhetlighet. Medlemsstaten bör i synnerhet utnämna en tillsynsmyndighet som fungerar som samlande kontaktpunkt för dessa myndigheters effektiva deltagande i mekanismen för att säkra ett snabbt och smidigt samarbete med övriga tillsynsmyndigheter, styrelsen och kommissionen.

(120) Varje tillsynsmyndighet bör tilldelas de ekonomiska och personella resurser och lokalutrymmen samt den infrastruktur som är nödvändig för att den effektivt ska kunna utföra sina uppgifter, däribland de uppgifter som är knutna till ömsesidigt bistånd och samarbete med övriga tillsynsmyndigheter i hela unionen. Varje tillsynsmyndighet bör ha en separat offentlig årlig budget, som kan ingå i den övergripande statsbudgeten eller nationella budgeten.

(121) De allmänna villkoren för tillsynsmyndighetens ledamot eller ledamöter bör fastställas genom varje medlemsstats lagstiftning och där bör i synnerhet föreskrivas att ledamöterna ska utnämnas genom ett öppet förfarande antingen av medlemsstatens parlament, regering eller statschef, på grundval av ett förslag från regeringen, en ledamot av regeringen, parlamentet eller en av parlamentets kammare eller av ett oberoende organ som enligt medlemsstaternas nationella rätt har anförtrotts utnämningen. I syfte att säkerställa tillsynsmyndighetens oberoende bör ledamoten eller ledamöterna handla med integritet, avstå från alla handlingar som står i strid med deras tjänsteutövning och under sin mandattid avstå från all annan avlönad eller oavlönad yrkesverksamhet som står i strid med deras uppdrag. Tillsynsmyndigheten bör ha egen personal, som valts ut av tillsynsmyndigheten eller ett oberoende organ som fastställs i medlemsstaternas nationella rätt, vilken uteslutande bör vara underställd tillsynsmyndighetens ledamot eller ledamöter.

(122) Varje tillsynsmyndighet bör ha behörighet att inom sin medlemsstats territorium utöva de befogenheter och utföra de uppgifter som den tilldelats i enlighet med denna förordning. Detta bör framför allt omfatta behandling

inom ramen för verksamhet vid den personuppgiftsansvariges eller personuppgiftsbiträdets verksamhetsställen inom den egna medlemsstatens territorium, behandling av personuppgifter som utförs av myndigheter eller privata organ som agerar i ett allmänt intresse, behandling som påverkar registrerade på dess territorium eller behandling som utförs av en personuppgiftsansvarig eller ett personuppgiftsbiträde som inte är etablerad i unionen när den rör registrerade som är bosatta på dess territorium. Detta bör inbegripa att hantera klagomål som lämnas in av en registrerad, genomföra undersökningar om tillämpningen av denna förordning samt främja allmänhetens medvetenhet om risker, bestämmelser, skyddsåtgärder och rättigheter när det gäller behandlingen av personuppgifter.

(123) Tillsynsmyndigheterna bör övervaka tillämpningen av bestämmelserna i denna förordning och bidra till att tillämpningen blir enhetlig över hela unionen, för att skydda fysiska personer vid behandling av deras personuppgifter och för att underlätta det fria flödet av personuppgifter inom den inre marknaden. För detta ändamål bör tillsynsmyndigheterna samarbeta såväl sinsemellan som med kommissionen, utan att det behövs något avtal mellan medlemsstaterna om tillhandahållande av ömsesidigt bistånd eller om sådant samarbete.

(124) Om behandlingen av personuppgifter sker inom ramen för verksamhet vid en personuppgiftsansvarigs eller ett personuppgiftsbiträdes verksamhetsställe i unionen och den personuppgiftsansvarige eller personuppgiftsbiträdet är etablerad i mer än en medlemsstat, eller om behandling som sker inom ramen för verksamhet vid ett enda verksamhetsställe tillhörande en personuppgiftsansvarig eller ett personuppgiftsbiträde i unionen i väsentlig grad påverkar eller sannolikt i väsentlig grad kommer att påverka registrerade i mer än en medlemsstat, bör tillsynsmyndigheten för den personuppgiftsansvariges eller personuppgiftsbiträdets huvudsakliga verksamhetsställe eller för detta enda verksamhetsställe tillhörande den personuppgiftsansvarige eller personuppgiftsbiträdet agera som ansvarig myndighet. Denna bör samarbeta med de övriga myndigheter som berörs, eftersom den personuppgiftsansvarige eller personuppgiftsbiträdet har ett verksamhetsställe inom deras medlemsstats territorium, eftersom registrerade som är bosatta på deras territorium i väsentlig grad påverkas eller eftersom ett klagomål har lämnats in till dem. Även när en registrerad som inte är bosatt i medlemsstaten har lämnat in ett klagomål, bör den tillsynsmyndighet som klagomålet har lämnats in till också vara en berörd tillsynsmyndighet. Styrelsen bör inom ramen för sina uppgifter kunna utfärda riktlinjer för alla frågor som rör tillämpningen av denna förordning, framför allt för vilka kriterier som ska beaktas för att konstatera om behandlingen i fråga i väsentlig grad påverkar registrerade i mer än en medlemsstat och för vad som utgör en relevant och motiverad invändning.

(125) Den ansvariga myndigheten bör ha behörighet att anta bindande beslut om åtgärder inom ramen för de befogenheter som den tilldelats i enlighet med denna förordning. I egenskap av ansvarig myndighet bör tillsynsmyndigheten nära involvera och samordna de berörda tillsynsmyndigheterna i beslutsfattandet. Om man beslutar att helt eller delvis avslå den registrerades klagomål, bör detta beslut antas av den tillsynsmyndighet som klagomålet har lämnats in till.

(126) Den ansvariga tillsynsmyndigheten och de berörda tillsynsmyndigheterna bör gemensamt enas om beslutet, som bör rikta sig till den personuppgiftsansvariges eller personuppgiftsbiträdets huvudsakliga eller enda verksamhetsställe och vara bindande för den personuppgiftsansvarige och personuppgiftsbiträdet. Den personuppgiftsansvarige eller personuppgiftsbiträdet bör vidta de åtgärder som krävs för att säkerställa efterlevnad av denna förordning och genomförande av det beslut som den ansvariga tillsynsmyndigheten har anmält till den personuppgiftsansvariges eller personuppgiftsbiträdets huvudsakliga verksamhetsställe vad gäller behandling i unionen.

(127) Varje tillsynsmyndighet som inte agerar som ansvarig tillsynsmyndighet bör vara behörig att behandla lokala fall, om den personuppgiftsansvarige eller personuppgiftsbiträdet är etablerad i mer än en medlemsstat men ärendet för den specifika behandlingen endast avser behandling som utförs i en enda medlemsstat och endast omfattar registrerade i denna enda medlemsstat, till exempel om ärendet avser behandling av anställdas personuppgifter inom ramen för en medlemsstats specifika anställningsförhållanden. I sådana fall bör tillsynsmyndigheten utan dröjsmål underrätta den ansvariga tillsynsmyndigheten om detta ärende. Efter att ha underrättats bör den ansvariga tillsynsmyndigheten besluta huruvida den kommer att hantera ärendet i enlighet med bestämmelsen om samarbete mellan den ansvariga tillsynsmyndigheten och andra berörda tillsynsmyndigheter (nedan kallad *mekanismen för en enda kontaktpunkt*), eller om den tillsynsmyndighet som underrättade den bör behandla ärendet på lokal nivå. När den ansvariga tillsynsmyndigheten beslutar huruvida den kommer att behandla ärendet, bör den ta hänsyn till om den personuppgiftsansvarige eller personuppgiftsbiträdet har ett verksamhetsställe i den medlemsstat där den tillsynsmyndighet som underrättade den ansvariga myndigheten är belägen för att säkerställa ett effektivt genomförande av ett beslut gentemot den personuppgiftsansvarige eller personuppgiftsbiträdet. När den ansvariga tillsynsmyndigheten beslutar att behandla ärendet, bör den tillsynsmyndighet som underrättade den

ha möjlighet att lämna in ett förslag till beslut, som den ansvariga tillsynsmyndigheten bör ta största möjliga hänsyn till när den utarbetar utkastet till beslut inom ramen för mekanismen för en enda kontaktpunkt.

(128) Bestämmelserna om den ansvariga tillsynsmyndigheten och mekanismen för en enda kontaktpunkt bör inte tillämpas om behandlingen utförs av myndigheter eller privata organ i ett allmänt intresse. I sådana fall bör den enda tillsynsmyndighet som är behörig att utöva de befogenheter som den tilldelas i enlighet med denna förordning vara tillsynsmyndigheten i den medlemsstat där myndigheten eller det privata organet är etablerat.

(129) För att denna förordning ska övervakas och verkställas på ett enhetligt sätt i hela unionen bör tillsynsmyndigheterna i alla medlemsstater ha samma uppgifter och effektiva befogenheter, bl.a. undersökningsbefogenheter, korrigerande befogenheter och befogenheter att ålägga sanktioner samt befogenheter att utfärda tillstånd och ge råd, särskilt vid klagomål från fysiska personer och, utan att det påverkar åklagarmyndigheternas befogenheter enligt medlemsstaternas nationella rätt, att upplysa de rättsliga myndigheterna om överträdelser av denna förordning och delta i rättsliga förfaranden. Dessa befogenheter bör även omfatta en befogenhet att införa en tillfällig eller definitiv begränsning av, inklusive förbud mot, behandling. Medlemsstaterna får fastställa andra uppgifter med anknytning till skyddet av personuppgifter enligt denna förordning. Tillsynsmyndigheternas befogenheter bör utövas opartiskt, rättvist och inom rimlig tid i överensstämmelse med lämpliga rättssäkerhetsgarantier i unionsrätten och i medlemsstaternas nationella rätt. Framför allt bör varje åtgärd vara lämplig, nödvändig och proportionell för att säkerställa efterlevnad av denna förordning, med beaktande av omständigheterna i varje enskilt fall, samt respektera varje persons rätt att bli hörd innan några enskilda åtgärder som påverkar honom eller henne negativt vidtas och vara utformad så att onödiga kostnader och alltför stora olägenheter för de berörda personerna undviks. Undersökningsbefogenheten när det gäller tillträde till lokaler bör utövas i enlighet med särskilda krav i medlemsstaternas nationella processrätt, såsom kravet på att inhämta förhandstillstånd från rättsliga myndigheter. Varje rättsligt bindande åtgärd som vidtas av tillsynsmyndigheten bör vara skriftlig, klar och entydig, innehålla information om vilken tillsynsmyndighet som har utfärdat åtgärden och datum för utfärdandet, vara undertecknad av tillsynsmyndighetens chef eller en av dess ledamöter efter dennes bemyndigande samt innehålla en motivering till åtgärden och en hänvisning till rätten till ett effektivt rättsmedel. Detta bör inte utesluta ytterligare krav enligt medlemsstaternas nationella processrätt. Antagande av ett rättsligt bindande beslut innebär att det kan bli föremål för domstolsprövning i den medlemsstat till vilken den tillsynsmyndighet som antog beslutet hör.

(130) Om den tillsynsmyndighet till vilken klagomålet har ingetts inte är den ansvariga tillsynsmyndigheten, bör den ansvariga tillsynsmyndigheten nära samarbeta med den tillsynsmyndighet till vilken klagomålet har ingetts i enlighet med de bestämmelser om samarbete och enhetlighet som fastställs i denna förordning. I sådana fall bör den ansvariga tillsynsmyndigheten när den vidtar åtgärder avsedda att ha rättsverkan, inbegripet utdömandet av administrativa sanktionsavgifter, ta största hänsyn till synpunkter från den tillsynsmyndighet till vilken klagomålet har ingetts, vilken bör kvarstå som behörig för genomförande av utredningar på den egna medlemsstatens territorium i samverkan med den behöriga tillsynsmyndigheten.

(131) Om en annan tillsynsmyndighet bör agera som ansvarig tillsynsmyndighet för den personuppgiftsansvariges eller personuppgiftsbiträdets behandling men den sakfråga som klagomålet gäller eller den möjliga överträdelsen endast rör den personuppgiftsansvariges eller personuppgiftsbiträdets behandling i den medlemsstat där klagomålet har ingetts eller den eventuella överträdelsen har upptäckts, och frågan inte i väsentlig grad påverkar eller inte sannolikt i väsentlig grad kommer att påverka registrerade i andra medlemsstater, bör den tillsynsmyndighet som mottar ett klagomål eller upptäcker eller på annat sätt informeras om situationer som innebär eventuella överträdelser av denna förordning försöka få till stånd en uppgörelse i godo med den personuppgiftsansvarige och, om detta inte lyckas, utöva sina befogenheter fullt ut. Detta bör omfatta särskild behandling som utförs inom tillsynsmyndighetens medlemsstats territorium eller med avseende på registrerade inom denna medlemsstats territorium, behandling som utförs inom ramen för ett erbjudande om varor eller tjänster som särskilt riktar sig till registrerade inom tillsynsmyndighetens medlemsstats territorium eller behandling som måste bedömas med beaktande av relevanta rättsliga skyldigheter enligt medlemsstaternas nationella rätt.

(132) Medvetandehöjande kampanjer från tillsynsmyndigheters sida riktade till allmänheten bör innefatta särskilda åtgärder riktade dels till personuppgiftsansvariga och personuppgiftsbiträden, inbegripet mikroföretag samt små och medelstora företag, dels till fysiska personer, särskilt i utbildningssammanhang.

(133) Tillsynsmyndigheterna bör hjälpa varandra att utföra sina uppgifter och ge ömsesidigt bistånd så att denna förordning tillämpas och verkställs enhetligt på den inre marknaden. En tillsynsmyndighet som begärt ömsesidigt bistånd får anta en provisorisk åtgärd, om den inte har fått något svar på en begäran om ömsesidigt bistånd inom en månad från det att begäran mottogs av den andra tillsynsmyndigheten.

(134) Alla tillsynsmyndigheter bör om lämpligt delta i gemensamma insatser med andra tillsynsmyndigheter. Den anmodade tillsynsmyndigheten bör vara skyldig att besvara en begäran inom en fastställd tidsperiod.

(135) För att denna förordning ska tillämpas enhetligt i hela unionen bör en mekanism för enhetlighet när det gäller samarbete mellan tillsynsmyndigheterna skapas. Denna mekanism bör främst tillämpas när en tillsynsmyndighet avser att anta en åtgärd som är avsedd att ha rättsverkan gällande behandlingar som i väsentlig grad påverkar ett betydande antal registrerade i flera medlemsstater. Den bör också tillämpas när en berörd tillsynsmyndighet eller kommissionen begär att ett sådant ärende ska hanteras inom ramen för mekanismen för enhetlighet. Mekanismen bör inte påverka åtgärder som kommissionen kan komma att vidta när den utövar sina befogenheter enligt fördragen.

(136) Vid tillämpningen av mekanismen för enhetlighet bör styrelsen inom en fastställd tidsperiod avge ett yttrande, om en majoritet av dess ledamöter så beslutar eller om någon berörd tillsynsmyndighet eller kommissionen begär detta. Styrelsen bör också ges befogenhet att anta rättsligt bindande beslut vid tvister mellan tillsynsmyndigheter. För detta ändamål bör den, normalt med två tredjedelars majoritet av sina ledamöter, utfärda rättsligt bindande beslut i tydligt fastställda fall då tillsynsmyndigheter har olika uppfattningar, framför allt när det gäller mekanismen för samarbete mellan den ansvariga tillsynsmyndigheten och berörda tillsynsmyndigheter om sakförhållandena, i synnerhet om huruvida denna förordning har överträtts.

(137) Det kan uppstå brådskande behov att agera för att skydda registrerades rättigheter och friheter, särskilt när fara föreligger att säkerställandet av en registrerad persons rättighet kan komma att försvåras avsevärt. En tillsynsmyndighet bör därför kunna vidta vederbörligen motiverade provisoriska åtgärder inom sitt territorium med en viss giltighetsperiod, som inte bör överskrida tre månader.

(138) Tillämpningen av en sådan mekanism bör vara ett villkor för lagligheten av en åtgärd som är avsedd att ha rättsverkan och som vidtas av tillsynsmyndigheten i de fall där denna tillämpning är obligatorisk. I andra ärenden som inbegriper flera länder bör samarbetsmekanismen mellan den ansvariga tillsynsmyndigheten och berörda tillsynsmyndigheter tillämpas, och ömsesidigt bistånd och gemensamma insatser kan utföras mellan de berörda tillsynsmyndigheterna på bilateral eller multilateral basis utan att mekanismen för enhetlighet utlöses.

(139) I syfte att främja en enhetlig tillämpning av denna förordning bör styrelsen inrättas som ett oberoende unionsorgan. För att styrelsen ska kunna uppfylla sina mål bör den vara en juridisk person. Styrelsen bör företrädas av sin ordförande. Den bör ersätta arbetsgruppen för skydd av fysiska personer med avseende på behandlingen av personuppgifter, som inrättades genom direktiv 95/46/EG. Den bör bestå av chefen för en tillsynsmyndighet i varje medlemsstat och Europeiska datatillsynsmannen eller deras respektive företrädare. Kommissionen bör delta i styrelsens verksamhet utan att ha rösträtt, och Europeiska datatillsynsmannen bör ha specifik rösträtt. Styrelsen bör bidra till denna förordnings enhetliga tillämpning i hela unionen, bl.a. genom att lämna råd till kommissionen, särskilt vad gäller skyddsnivån i tredjeländer eller internationella organisationer, och främja samarbetet mellan tillsynsmyndigheterna i hela unionen. Styrelsen bör agera oberoende när den utför sina uppgifter.

(140) Styrelsen bör biträdas av ett sekretariat som tillhandahålls av Europeiska datatillsynsmannen. Den personal vid Europeiska datatillsynsmannen som medverkar i utförandet av de uppgifter som enligt denna förordning anförtros styrelsen bör för sina uppgifter uteslutande ta emot instruktioner från styrelsens ordförande och rapportera till denne.

(141) Alla registrerade bör ha rätt att lämna in ett klagomål till en enda tillsynsmyndighet, särskilt i den medlemsstat där den registrerade har sin hemvist, och ha rätt till ett effektivt rättsmedel i enlighet med artikel 47 i stadgan,

om den registrerade anser att hans eller hennes rättigheter enligt denna förordning har kränkts eller om tillsynsmyndigheten inte reagerar på ett klagomål, helt eller delvis avslår eller avvisar ett klagomål eller inte agerar när så är nödvändigt för att skydda den registrerades rättigheter. Utredningen av ett klagomål bör, med förbehåll för eventuell domstolsprövning, ske i den utsträckning som är lämplig i det enskilda fallet. Tillsynsmyndigheten bör inom rimlig tid informera den registrerade om hur arbetet med klagomålet fortskrider och vad resultatet blir. Om ärendet fordrar ytterligare utredning eller samordning med en annan tillsynsmyndighet, bör den registrerade underrättas även om detta. För att förenkla inlämningen av klagomål bör varje tillsynsmyndighet vidta åtgärder, såsom att tillhandahålla ett formulär för inlämnande av klagomål som även kan fyllas i elektroniskt, utan att andra kommunikationsformer utesluts.

(142) Om en registrerad anser att hans eller hennes rättigheter enligt denna förordning har kränkts, bör han eller hon ha rätt att ge mandat till ett organ, en organisation eller en sammanslutning som drivs utan vinstsyfte och som har inrättats i enlighet med en medlemsstats nationella rätt, som har stadgeenliga mål av allmänt intresse och bedriver verksamhet på området skydd av personuppgifter, att på hans eller hennes vägnar lämna in ett klagomål till en tillsynsmyndighet, om detta föreskrivs i medlemsstatens nationella rätt, att på den registrerades vägnar utöva rätten till domstolsprövning eller att på den registrerades vägnar utöva rätten att ta emot ersättning. En medlemsstat får föreskriva att ett sådant organ, en sådan organisation eller en sådan sammanslutning ska ha rätt att lämna in ett klagomål i den medlemsstaten, oberoende av en registrerad persons mandat, och ha rätt till ett effektivt rättsmedel, om det eller den har skäl att anse att en registrerad persons rättigheter har kränkts till följd av behandling av personuppgifter som strider mot denna förordning. Detta organ, denna organisation eller denna sammanslutning får inte ges rätt att kräva ersättning på en registrerad persons vägnar oberoende av den registrerades mandat.

(143) Varje fysisk eller juridisk person har rätt att väcka ogiltighetstalan mot styrelsens beslut vid domstolen enligt de villkor som föreskrivs i artikel 263 i EUF-fördraget. I sin egenskap av adressater för sådana beslut måste, i enlighet med artikel 263 i EUF-fördraget, de berörda tillsynsmyndigheter som önskar överklaga dessa väcka talan inom två månader efter det att beslutet meddelats dem. Om styrelsens beslut direkt och personligen berör en personuppgiftsansvarig, ett personuppgiftsbiträde eller en enskild, kan den enskilde väcka ogiltighetstalan mot besluten inom två månader efter det att de har offentliggjorts på styrelsens webbplats, i enlighet med artikel 263 i EUF-fördraget. Utan att det påverkar denna rätt inom ramen för artikel 263 i EUF-fördraget bör varje fysisk eller juridisk person ha rätt till ett effektivt rättsmedel vid den behöriga nationella domstolen mot ett beslut av en tillsynsmyndighet som har rättsliga följder för denna person. Sådana beslut avser särskilt tillsynsmyndighetens utövande av utrednings-, korrigerings- och godkännandebefogenheter eller avvisande av eller avslag på klagomål. Rätten till ett effektivt rättsmedel inbegriper dock inte åtgärder som vidtagits av tillsynsmyndigheter när dessa inte är rättsligt bindande, såsom yttranden som avgivits eller rådgivning som tillhandahållits av tillsynsmyndigheten. Talan mot beslut som har fattats av en tillsynsmyndighet bör väckas vid domstolarna i den medlemsstat där tillsynsmyndigheten har sitt säte och bör genomföras i enlighet med den medlemsstatens nationella processrätt. Dessa domstolar bör ha fullständig behörighet, vilket bör omfatta behörighet att pröva alla fakta och rättsliga frågor som rör den tvist som anhängiggjorts vid dem.

Om talan avslås eller avvisas av en tillsynsmyndighet, kan den enskilde väcka talan vid domstolarna i samma medlemsstat. I samband med rättsmedel som avser tillämpningen av denna förordning kan eller, i det fall som anges i artikel 267 i EUF-fördraget, måste nationella domstolar som anser att ett beslut om ett förhandsavgörande är nödvändigt för att de ska kunna döma begära att domstolen meddelar ett förhandsavgörande om tolkningen av unionsrätten, inbegripet denna förordning. Om dessutom ett beslut av en tillsynsmyndighet om genomförande av ett beslut av styrelsen överklagas till en nationell domstol och giltigheten av styrelsens beslut ifrågasätts, har inte den nationella domstolen befogenhet att förklara styrelsens beslut ogiltigt utan måste hänskjuta frågan om giltighet till domstolen i enlighet med artikel 267 i EUF-fördraget såsom den tolkats av domstolen, närhelst den anser att beslutet är ogiltigt. En nationell domstol får dock inte hänskjuta en fråga om giltigheten av styrelsens beslut på begäran av en fysisk eller juridisk person som haft tillfälle att väcka ogiltighetstalan mot beslutet, i synnerhet inte om denna person direkt och personligen berördes av beslutet men inte gjorde detta inom den frist som anges i artikel 263 i EUF-fördraget.

(144) Om en domstol där ett förfarande inletts mot beslut som har fattats av en tillsynsmyndighet har skäl att tro att ett förfarande rörande samma behandling, såsom samma sakfråga vad gäller behandling av samma personuppgiftsansvarige eller samma personuppgiftsbiträde, eller samma händelseförlopp, har inletts vid en annan behörig domstol i en annan medlemsstat, bör den kontakta denna domstol i syfte att bekräfta förekomsten av sådana relaterade förfaranden. Om relaterade förfaranden pågår vid en domstol i en annan medlemsstat får alla andra

domstolar än den domstol där förfarandet först inleddes låta förfarandena vila eller på en av parternas begäran förklara sig obehöriga till förmån för den domstol där förfarandet först inleddes, om den domstolen har behörighet i förfarandet i fråga och dess lagstiftning tillåter förening av sådana relaterade förfaranden. Förfarandena anses vara relaterade, om de är så nära förenade att en gemensam handläggning och dom är påkallad för att undvika att oförenliga domar meddelas som en följd av att förfarandena prövas i olika rättegångar.

(145) När det gäller ett rättsligt förfarande mot en personuppgiftsansvarig eller ett personuppgiftsbiträde bör käranden kunna välja att väcka talan antingen vid domstolarna i de medlemsstater där den personuppgiftsansvarige eller personuppgiftsbiträdet är etablerad eller där den registrerade är bosatt, såvida inte den personuppgiftsansvarige är en myndighet i en medlemsstat som agerar inom ramen för sin myndighetsutövning.

(146) Den personuppgiftsansvarige eller personuppgiftsbiträdet bör ersätta all skada som en person kan komma att lida till följd av behandling som strider mot denna förordning. Den personuppgiftsansvarige eller personuppgiftsbiträdet bör dock befrias från skadeståndsskyldighet om den kan visa att den inte på något sätt är ansvarig för skadan. Begreppet skada bör tolkas brett mot bakgrund av domstolens rättspraxis på ett sätt som fullt ut återspeglar denna förordnings mål. Detta påverkar inte skadeståndsanspråk till följd av överträdelser av andra bestämmelser i unionsrätten eller i medlemsstaternas nationella rätt. Behandling som strider mot denna förordning omfattar även behandling som strider mot delegerade akter och genomförandeakter som antagits i enlighet med denna förordning och medlemsstaternas nationella rätt med närmare specifikation av denna förordnings bestämmelser. Registrerade bör få full och effektiv ersättning för den skada de lidit. Om personuppgiftsansvariga eller personuppgiftsbiträden medverkat vid samma behandling, bör varje personuppgiftsansvarig eller personuppgiftsbiträde hållas ansvarig för hela skadan. Om de är förenade i samma rättsliga förfarande i enlighet med medlemsstaternas nationella rätt, kan ersättningen dock fördelas i enlighet med varje personuppgiftsansvarigs eller personuppgiftsbiträdes ansvar för den genom behandlingen uppkomna skadan, förutsatt att den registrerade som lidit skada tillförsäkras full och effektiv ersättning. Varje personuppgiftsansvarig eller personuppgiftsbiträde som har betalat full ersättning får därefter inleda förfaranden för återkrav mot andra personuppgiftsansvariga eller personuppgiftsbiträden som medverkat vid samma behandling.

(147) Om särskilda bestämmelser om behörighet fastställs i denna förordning, framför allt vad gäller förfaranden för att begära rättslig prövning som inbegriper ersättning mot en personuppgiftsansvarig eller ett personuppgiftsbiträde, bör inte allmänna bestämmelser om behörighet, såsom bestämmelserna i Europaparlamentets och rådets förordning (EU) nr 1215/2012 [1], påverka tillämpningen av sådana särskilda bestämmelser.

(148) För att stärka verkställigheten av denna förordning bör det utdömas sanktioner, inbegripet administrativa sanktionsavgifter, för överträdelser av denna förordning utöver eller i stället för de lämpliga åtgärder som tillsynsmyndigheten vidtar i enlighet med denna förordning. Vid en mindre överträdelse eller om den sanktionsavgift som sannolikt skulle utdömas skulle innebära en oproportionell börda för en fysisk person får en reprimand utfärdas i stället för sanktionsavgifter. Vederbörlig hänsyn bör dock tas till överträdelsens karaktär, svårighetsgrad och varaktighet och huruvida den har skett uppsåtligen, vilka åtgärder som vidtagits för att lindra skadan, graden av ansvar eller eventuella tidigare överträdelser av relevans, det sätt på vilket överträdelsen kom till tillsynsmyndighetens kännedom, efterlevnad av åtgärder som förordnats mot den personuppgiftsansvarige eller personuppgiftsbiträdet, tillämpning av en uppförandekod och eventuella andra försvårande eller förmildrande faktorer. Utdömandet av sanktioner, inbegripet administrativa sanktionsavgifter, bör underkastas adekvata rättssäkerhetsgarantier i överensstämmelse med allmänna principer inom unionsrätten och stadgan, vilket inbegriper ett effektivt rättsligt skydd och korrekt rättsligt förfarande.

(149) Medlemsstaterna bör kunna fastställa bestämmelser om straffrättsliga påföljder för överträdelser av denna förordning, inbegripet för överträdelser av nationella bestämmelser som antagits i enlighet med och inom ramen för denna förordning. Dessa straffrättsliga påföljder kan även inbegripa en möjlighet att förverka den vinning som gjorts genom överträdelser av denna förordning. Utdömandet av straffrättsliga påföljder för överträdelser av sådana nationella bestämmelser och administrativa sanktioner bör dock inte medföra ett åsidosättande av principen ne bis in idem enligt domstolens tolkning.

(150) För att förstärka och harmonisera de administrativa sanktionerna för överträdelser av denna förordning bör samtliga tillsynsmyndigheter ha befogenhet att utfärda administrativa sanktionsavgifter. Det bör i denna

[1] Europaparlamentets och rådets förordning (EU) nr 1215/2012 av den 12 december 2012 om domstols behörighet och om erkännande och verkställighet av domar på privaträttens område (EUT L 351, 20.12.2012, s. 1).

förordning anges vilka överträdelserna är, den övre gränsen för och kriterierna för fastställande av de administrativa sanktionsavgifterna, som i varje enskilt fall bör bestämmas av den behöriga tillsynsmyndigheten med beaktande av alla relevanta omständigheter i det särskilda fallet, med vederbörlig hänsyn bl.a. till överträdelsens karaktär, svårighetsgrad och varaktighet samt till dess följder och till de åtgärder som vidtas för att sörja för fullgörandet av skyldigheterna enligt denna förordning och för att förebygga eller lindra konsekvenserna av överträdelsen. Om de administrativa sanktionsavgifterna åläggs ett företag, bör ett företag i detta syfte anses vara ett företag i den mening som avses i artiklarna 101 och 102 i EUF-fördraget. Om de administrativa sanktionsavgifterna åläggs personer som inte är ett företag, bör tillsynsmyndigheten ta hänsyn till den allmänna inkomstnivån i medlemsstaten och personens ekonomiska situation, när den överväger lämplig sanktionsavgift. Mekanismen för enhetlighet kan också tillämpas för att främja en enhetlig tillämpning av administrativa sanktionsavgifter. Medlemsstaterna bör fastställa om och i vilken utsträckning myndigheter ska omfattas av administrativa sanktionsavgifter. Utfärdande av administrativa sanktionsavgifter eller utdelning av en varning påverkar inte tillämpningen av tillsynsmyndigheternas övriga befogenheter eller av andra sanktioner enligt denna förordning.

(151) Danmarks och Estlands rättssystem tillåter inte administrativa sanktionsavgifter i enlighet med denna förordning. Bestämmelserna om administrativa sanktionsavgifter kan tillämpas så att sanktionsavgiften i Danmark utdöms som en straffrättslig påföljd av en behörig nationell domstol och att den i Estland utdöms av tillsynsmyndigheten inom ramen för ett förseelseförfarande, under förutsättning att en sådan tillämpning av bestämmelserna i dessa medlemsstater har en effekt som är likvärdig med administrativa sanktionsavgifter som utdöms av tillsynsmyndigheter. De behöriga nationella domstolarna bör därför beakta rekommendationen från den tillsynsmyndighet som initierar sanktionsavgiften. De sanktionsavgifter som utdöms bör i alla händelser vara effektiva, proportionella och avskräckande.

(152) Om denna förordning inte harmoniserar administrativa sanktioner eller om nödvändigt i andra fall, till exempel vid fall av allvarliga överträdelser av denna förordning, bör medlemsstaterna genomföra ett system med effektiva, proportionella och avskräckande sanktioner. Dessa sanktioners art, straffrättsliga eller administrativa, bör fastställas i medlemsstaternas nationella rätt.

(153) Medlemsstaterna bör i sin lagstiftning sammanjämka bestämmelserna om yttrandefrihet och informationsfrihet, vilket inbegriper journalistiska, akademiska, konstnärliga och/eller litterära uttrycksformer, med rätten till skydd av personuppgifter i enlighet med denna förordning. Behandling av personuppgifter enbart för journalistiska, akademiska, konstnärliga eller litterära ändamål bör undantas från vissa av kraven i denna förordning, så att rätten till skydd av personuppgifter vid behov kan förenas med rätten till yttrandefrihet och informationsfrihet, som följer av artikel 11 i stadgan. Detta bör särskilt gälla vid behandling av personuppgifter inom det audiovisuella området och i nyhetsarkiv och pressbibliotek. Medlemsstaterna bör därför anta lagstiftningsåtgärder som fastställer de olika undantag som behövs för att skapa en balans mellan dessa grundläggande rättigheter. Medlemsstaterna bör fastställa sådana undantag med avseende på allmänna principer, de registrerades rättigheter, personuppgiftsansvariga och personuppgiftsbiträden, överföring av uppgifter till tredjeländer eller internationella organisationer, de oberoende tillsynsmyndigheterna, samarbete och enhetlighet samt specifika situationer där personuppgifter behandlas. Om sådana undantag varierar från en medlemsstat till en annan, ska den nationella rätten i den medlemsstat vars lag den personuppgiftsansvarige omfattas av tillämpas. För att beakta vikten av rätten till yttrandefrihet i varje demokratiskt samhälle måste det göras en bred tolkning av vad som innefattas i denna frihet, som till exempel journalistik.

(154) Denna förordning gör det möjligt att vid tillämpningen av den ta hänsyn till principen om allmänhetens rätt att få tillgång till allmänna handlingar. Allmänhetens rätt att få tillgång till allmänna handlingar kan betraktas som ett allmänt intresse. Personuppgifter i handlingar som innehas av en myndighet eller ett offentligt organ bör kunna lämnas ut offentligt av denna myndighet eller detta organ, om utlämning stadgas i unionsrätten eller i medlemsstatens nationella rätt som är tillämplig på myndigheten eller det offentliga organet. Denna rätt bör sammanjämka allmänhetens rätt att få tillgång till allmänna handlingar och vidareutnyttjande av information från den offentliga sektorn med rätten till skydd av personuppgifter och får därför innehålla föreskrifter om den nödvändiga sammanjämkningen med rätten till skydd av personuppgifter enligt denna förordning. Hänvisningen till offentliga myndigheter och organ bör i detta sammanhang omfatta samtliga myndigheter eller andra organ som omfattas av medlemsstaternas nationella rätt om allmänhetens tillgång till handlingar. Europaparlamentets och rådets direktiv 2003/98/EG ([1]) ska inte på något sätt påverka skyddsnivån för fysiska personer med avseende

([1]) Europaparlamentets och rådets direktiv 2003/98/EG av den 17 november 2003 om vidareutnyttjande av information från den offentliga sektorn (EUT L 345, 31.12.2003, s. 90).

på behandling av personuppgifter enligt bestämmelserna i unionsrätten och i medlemsstaternas nationella rätt och i synnerhet ändras inte de skyldigheter och rättigheter som anges i denna förordning genom det direktivet. I synnerhet ska direktivet inte vara tillämpligt på handlingar till vilka, med hänsyn till skyddet av personuppgifter, tillgång enligt tillgångsbestämmelserna är utesluten eller begränsad eller på delar av handlingar som är tillgängliga enligt dessa bestämmelser men som innehåller personuppgifter vilkas vidareutnyttjande i lag har fastställts som oförenligt med lagstiftningen om skydd för fysiska personer vid behandling av personuppgifter.

(155) En medlemsstatsnationella rätt eller kollektivavtal, inbegripet ”verksamhetsöverenskommelser”, får föreskriva särskilda bestämmelser om behandling av anställdas personuppgifter i anställningsförhållanden, särskilt när det gäller villkoren för hur personuppgifter i anställningsförhållanden får behandlas på grundval av samtycke från den anställde, rekrytering, genomförande av anställningsavtalet, inklusive befrielse från i lag eller kollektivavtal stadgade skyldigheter, ledning, planering och organisering av arbetet samt hälsa och säkerhet på arbetsplatsen, men också när det gäller att såväl kollektivt som individuellt utöva och komma i åtnjutande av rättigheter och förmåner som är knutna till anställningen samt att avsluta anställningsförhållandet.

(156) Behandlingen av personuppgifter för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål bör omfattas av lämpliga skyddsåtgärder för de registrerades rättigheter och friheter enligt denna förordning. Skyddsåtgärderna bör säkerställa att tekniska och organisatoriska åtgärder har införts för att se till att särskilt principen om uppgiftsminimering iakttas. Ytterligare behandling av personuppgifter för arkivändamål av allmänintresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål bör genomföras, när den personuppgiftsansvarige har bedömt möjligheten att uppnå dessa ändamål genom behandling av personuppgifter som inte medger eller inte längre medger identifiering av de registrerade, förutsatt att det finns lämpliga skyddsåtgärder (t. ex. pseudonymisering av personuppgifter). Medlemsstaterna bör införa lämpliga skyddsåtgärder för behandlingen av personuppgifter för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål. Medlemsstaterna bör på särskilda villkor med förbehåll för lämpliga skyddsåtgärder för de registrerade ha rätt att specificera och göra undantag från kraven på information, rätten till rättelse eller radering av personuppgifter, rätten att bli bortglömd, rätten till begränsning av behandlingen, rätten till dataportabilitet och rätten att göra invändning i samband med behandling av personuppgifter för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål. Villkoren och säkerhetsåtgärderna i fråga kan medföra att de registrerade måste följa särskilda förfaranden för att utöva dessa rättigheter, om det är lämpligt med hänsyn till den särskilda behandlingens syfte tillsammans med tekniska och organisatoriska åtgärder som syftar till att minimera behandlingen av personuppgifter i enlighet med principerna om proportionalitet och nödvändighet. Behandling av personuppgifter för vetenskapliga ändamål bör även vara förenlig med annan relevant lagstiftning, exempelvis om kliniska prövningar.

(157) Genom att koppla samman information från olika register kan forskare erhålla ny kunskap av stort värde med avseende på medicinska tillstånd som exempelvis hjärt-kärlsjukdomar, cancer och depression. På grundval av registren kan forskningsresultaten förbättras, eftersom de bygger på en större befolkningsgrupp. Forskning inom samhällsvetenskap som bedrivs på grundval av register gör det möjligt för forskare att få grundläggande kunskaper om sambandet på lång sikt mellan ett antal sociala villkor, exempelvis arbetslöshet och utbildning, och andra livsförhållanden. Forskningsresultat som erhållits på grundval av register utgör en stabil, högkvalitativ kunskap, som kan ligga till grund för utformningen och genomförandet av kunskapsbaserad politik, förbättra livskvaliteten för ett antal personer och förbättra de sociala tjänsternas effektivitet. För att underlätta vetenskaplig forskning får personuppgifter behandlas för vetenskapliga forskningsändamål, med förbehåll för lämpliga villkor och skyddsåtgärder i unionsrätten eller i medlemsstaternas nationella rätt.

(158) Om personuppgifter behandlas för arkivändamål, bör denna förordning också gälla denna behandling, med beaktande av att denna förordning inte bör gälla för avlidna personer. Offentliga myndigheter eller offentliga eller privata organ som innehar uppgifter av allmänt intresse bör vara tillhandahållare som, i enlighet med unionsrätten eller medlemsstaternas nationella rätt, har en rättslig skyldighet att förvärva, bevara, bedöma, organisera, beskriva, kommunicera, främja, sprida och ge tillgång till uppgifter av bestående värde för allmänintresset. Medlemsstaterna bör också ha rätt att föreskriva att personuppgifter får vidarebehandlas för arkivering, exempelvis i syfte att tillhandahålla specifik information om politiskt beteende under tidigare totalitära regimer, folkmord, brott mot mänskligheten, särskilt Förintelsen, eller krigsförbrytelser.

(159) Om personuppgifter behandlas för vetenskapliga forskningsändamål, bör denna förordning också gälla denna behandling. Behandling av personuppgifter för vetenskapliga forskningsändamål bör i denna förordning ges en vid tolkning och omfatta till exempel teknisk utveckling och demonstration, grundforskning, tillämpad forskning och privatfinansierad forskning. Behandlingen av personuppgifter bör dessutom ta hänsyn till unionens mål enligt artikel 179.1 i EUF-fördraget angående åstadkommandet av ett europeiskt forskningsområde. Vetenskapliga forskningsändamål bör också omfatta studier som utförs av ett allmänt intresse inom folkhälsoområdet. För att tillgodose de särskilda kraven i samband med behandling av personuppgifter för vetenskapliga forskningsändamål bör särskilda villkor gälla, särskilt vad avser offentliggörande eller annat utlämnande av personuppgifter inom ramen för vetenskapliga forskningsändamål. Om resultatet av vetenskaplig forskning, särskilt för hälso- och sjukvårdsändamål, ger anledning till ytterligare åtgärder i den registrerades intresse, bör de allmänna reglerna i denna förordning tillämpas på dessa åtgärder.

(160) Om personuppgifter behandlas för historiska forskningsändamål, bör denna förordning också gälla denna behandling. Detta bör även omfatta forskning för historiska och genealogiska ändamål, med beaktande av att denna förordning inte bör gälla för avlidna personer.

(161) När det gäller samtycke till deltagande i vetenskaplig forskning inom ramen för kliniska prövningar, bör de relevanta bestämmelserna i Europaparlamentets och rådets förordning (EU) nr 536/2014 ([1]) tillämpas.

(162) Om personuppgifter behandlas för statistiska ändamål, bör denna förordning gälla denna behandling. Unionsrätten eller medlemsstaternas nationella rätt bör, inom ramen för denna förordning, fastställa statistiskt innehåll, kontroll av tillgång, specifikationer för behandling av personuppgifter för statistiska ändamål och lämpliga åtgärder till skydd för den registrerades rättigheter och friheter och för att säkerställa insynsskydd för statistiska uppgifter. Med statistiska ändamål avses varje åtgärd som vidtas för den insamling och behandling av personuppgifter som är nödvändig för statistiska undersökningar eller för framställning av statistiska resultat. Dessa statistiska resultat kan vidare användas för olika ändamål, inbegripet vetenskapliga forskningsändamål. Ett statistiskt ändamål innebär att resultatet av behandlingen för statistiska ändamål inte består av personuppgifter, utan av aggregerade personuppgifter, och att resultatet eller uppgifterna inte används till stöd för åtgärder eller beslut som avser en särskild fysiskperson.

(163) De konfidentiella uppgifter som unionens myndigheter och nationella statistikansvariga myndigheter samlar in för att framställa officiell europeisk och officiell nationell statistik bör skyddas. Europeisk statistik bör utvecklas, framställas och spridas i enlighet med de statistiska principerna i artikel 338.2 i EUF-fördraget, medan hanteringen av nationell statistik även bör överensstämma med medlemsstaternas nationella rätt. Europaparlamentets och rådets förordning (EG) nr 223/2009 ([2]) innehåller ytterligare preciseringar om statistisk konfidentialitet för europeisk statistik.

(164) Vad beträffar tillsynsmyndigheternas befogenheter att från personuppgiftsansvariga eller personuppgiftsbiträden få tillgång till personuppgifter och tillträde till lokaler, får medlemsstaterna, inom gränserna för denna förordning, genom lagstiftning anta särskilda regler för att skydda yrkesmässig eller annan motsvarande tystnadsplikt, i den mån detta är nödvändigt för att jämka samman rätten till skydd av personuppgifter med tystnadsplikten. Detta påverkar inte tillämpningen av medlemsstaternas befintliga skyldigheter att anta bestämmelser om tystnadsplikt, där detta krävs enligt unionsrätten.

(165) Denna förordning är förenlig med kravet på att respektera och inte påverka den ställning som kyrkor och religiösa sammanslutningar eller samfund har i medlemsstaterna enligt gällande grundlag i enlighet med artikel 17 i EUF-fördraget.

(166) I syfte att uppnå målen för denna förordning, nämligen att skydda fysiska personers grundläggande rättigheter och friheter och i synnerhet deras rätt till skydd av personuppgifter och för att säkra det fria flödet av

([1]) Europaparlamentets och rådets förordning (EU) nr 536/2014 av den 16 april 2014 om kliniska prövningar av humanläkemedel och om upphävande av direktiv 2001/20/EG (EUT L 158, 27.5.2014, s. 1).

([2]) Europaparlamentets och rådets förordning (EG) nr 223/2009 av den 11 mars 2009 om europeisk statistik och om upphävande av Europaparlamentets och rådets förordning (EG, Euratom) nr 1101/2008 om utlämnande av insynsskyddade statistiska uppgifter till Europeiska gemenskapernas statistikkontor, rådets förordning (EG) nr 322/97 om gemenskapsstatistik och rådets beslut 89/382/EEG, Euratom om inrättande av en kommitté för Europeiska gemenskapernas statistiska program (EUT L 87, 31.3.2009, s. 164).

personuppgifter inom unionen, bör befogenheten att anta akter i enlighet med artikel 290 i EUF-fördraget delegeras till kommissionen. Delegerade akter bör framför allt antas när det gäller kriterier och krav vad gäller certifieringsmekanismer, information som ska ges med användning av standardiserade symboler och förfaranden för att tillhandahålla sådana symboler. Det är särskilt viktigt att kommissionen genomför lämpliga samråd under sitt förberedande arbete, inklusive på expertnivå. När kommissionen förbereder och utarbetar delegerade akter bör den se till att relevanta handlingar översänds samtidigt till Europaparlamentet och rådet och att detta sker så snabbt som möjligt och på lämpligt sätt.

(167) För att säkerställa enhetliga villkor för tillämpningen av denna förordning bör kommissionen ges genomförandebefogenheter i enlighet med denna förordning. Dessa befogenheter bör utövas i enlighet med förordning (EU) nr 182/2011. Kommissionen bör därvid överväga särskilda åtgärder för mikroföretag och små och medelstora företag.

(168) Granskningsförfarandet bör användas vid antagande av genomförandeakter om standardavtalsklausuler mellan personuppgiftsansvariga och personuppgiftsbiträden och mellan personuppgiftsbiträden, uppförandekoder, tekniska standarder och mekanismer för certifiering, adekvat nivå på det skydd som lämnas av ett tredjeland, ett territorium eller av en specificerad sektor inom det tredjelandet eller en internationell organisation, standardiserade skyddsbestämmelser, format och förfaranden för elektroniskt utbyte av information mellan personuppgiftsansvariga, personuppgiftsbiträden och tillsynsmyndigheter för bindande företagsbestämmelser, ömsesidigt bistånd och tillvägagångssätt för elektroniskt utbyte av information mellan tillsynsmyndigheter samt mellan tillsynsmyndigheter och styrelsen.

(169) Kommissionen bör när det föreligger tvingande skäl till skyndsamhet anta omedelbart tillämpliga genomförandeakter, när tillgängliga bevis visar att ett tredjeland, ett territorium eller en specificerad sektor inom det tredjelandet eller en internationell organisation inte upprätthåller en adekvat skyddsnivå.

(170) Eftersom målet för denna förordning, nämligen att säkerställa en likvärdig nivå för skyddet av fysiska personer och det fria flödet av personuppgifter inom hela unionen, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna utan snarare, på grund av åtgärdens omfattning eller verkningar, kan uppnås bättre på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget om Europeiska unionen (EU-fördraget). I enlighet med proportionalitetsprincipen i samma artikel går denna förordning inte utöver vad som är nödvändigt för att uppnå detta mål.

(171) Direktiv 95/46/EG bör upphävas genom denna förordning. Behandling som redan pågår den dag då denna förordning börjar tillämpas bör bringas i överensstämmelse med denna förordning inom en period av två år från det att denna förordning träder i kraft. Om behandlingen grundar sig på samtycke enligt direktiv 95/46/EG, är det inte nödvändigt att den registrerade på nytt ger sitt samtycke för att den personuppgiftsansvarige ska kunna fortsätta med behandlingen i fråga efter det att denna förordning börjar tillämpas, om det sätt på vilket samtycket gavs överensstämmer med villkoren i denna förordning. Beslut av kommissionen som antagits och tillstånd från tillsynsmyndigheterna som utfärdats på grundval av direktiv 95/46/EG ska fortsatt vara giltiga tills de ändras, ersätts eller upphävs.

(172) Europeiska datatillsynsmannen har hörts i enlighet med artikel 28.2 i förordning (EG) nr 45/2001 och avgav ett yttrande den 7 mars 2012 ([1]).

(173) Denna förordning bör vara tillämplig på alla frågor som gäller skyddet av grundläggande rättigheter och friheter i förhållande till behandlingen av personuppgifter, vilka inte omfattas av särskilda skyldigheter med samma mål som anges i Europaparlamentets och rådets direktiv 2002/58/EG ([2]), däribland den personuppgiftsansvariges skyldigheter och fysiska personers rättigheter. För att klargöra förhållandet mellan denna förordning och direktiv 2002/58/EG bör det direktivet ändras. När denna förordning har antagits, bör direktiv 2002/58/EG ses över, framför allt för att säkerställa konsekvens med denna förordning.

([1]) EUT C 192, 30.6.2012, s. 7.

([2]) Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation) (EGT L 201, 31.7.2002, s. 37).

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL I

Allmänna bestämmelser

Artikel 1

Syfte

1. I denna förordning fastställs bestämmelser om skydd för fysiska personer med avseende på behandlingen av personuppgifter och om det fria flödet av personuppgifter.

2. Denna förordning skyddar fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter.

3. Det fria flödet av personuppgifter inom unionen får varken begränsas eller förbjudas av skäl som rör skyddet för fysiska personer med avseende på behandlingen av personuppgifter.

Artikel 2

Materiellt tillämpningsområde

1. Denna förordning ska tillämpas på sådan behandling av personuppgifter som helt eller delvis företas på automatisk väg samt på annan behandling än automatisk av personuppgifter som ingår i eller kommer att ingå i ett register.

2. Denna förordning ska inte tillämpas på behandling av personuppgifter som

a) utgör ett led i en verksamhet som inte omfattas av unionsrätten,

b) medlemsstaterna utför när de bedriver verksamhet som omfattas av avdelning V kapitel 2 i EU-fördraget,

c) en fysisk person utför som ett led i verksamhet av rent privat natur eller som har samband med hans eller hennes hushåll,

d) behöriga myndigheter utför i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, i vilket även ingår att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten.

3. Förordning (EG) nr 45/2001 är tillämplig på den behandling av personuppgifter som sker i EU:s institutioner, organ och byråer. Förordning (EG) nr 45/2001 och de av unionens övriga rättsakter som är tillämpliga på sådan behandling av personuppgifter ska anpassas till principerna och bestämmelserna i denna förordning i enlighet med artikel 98.

4. Denna förordning påverkar inte tillämpningen av direktiv 2000/31/EG, särskilt bestämmelserna om tjänsteleverera nde mellanhänders ansvar i artiklarna 12–15 i det direktivet.

Artikel 3

Territoriellt tillämpningsområde

1. Denna förordning ska tillämpas på behandlingen av personuppgifter inom ramen för den verksamhet som bedrivs av en personuppgiftsansvarig eller ett personuppgiftsbiträde som är etablerad i unionen, oavsett om behandlingen utförs i unionen eller inte.

2. Denna förordning ska tillämpas på behandling av personuppgifter som avser registrerade som befinner sig i unionen och som utförs av en personuppgiftsansvarig eller ett personuppgiftsbiträde som inte är etablerad i unionen, om behandlingen har anknytning till

a) utbjudande av varor eller tjänster till sådana registrerade i unionen, oavsett om dessa varor eller tjänster erbjuds kostnadsfritt eller inte, eller

b) övervakning av deras beteende så länge beteendet sker inom unionen.

3. Denna förordning ska tillämpas på behandling av personuppgifter som utförs av en personuppgiftsansvarig som inte är etablerad i unionen, men på en plats där en medlemsstats nationella rätt gäller enligt folkrätten.

Artikel 4

Definitioner

I denna förordning avses med

1. *personuppgifter*: varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad *en registrerad*), varvid en identifierbarfysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet,

2. *behandling*: en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring,

3. *begränsning av behandling*: markering av lagrade personuppgifter med syftet att begränsa behandlingen av dessa i framtiden,

4. *profilering*: varje form av automatisk behandling av personuppgifter som består i att dessa personuppgifter används för att bedöma vissa personliga egenskaper hos en fysisk person, i synnerhet för att analysera eller förutsäga denna fysiska persons arbetsprestationer, ekonomiska situation, hälsa, personliga preferenser, intressen, pålitlighet, beteende, vistelseort eller förflyttningar,

5. *pseudonymisering*: behandling av personuppgifter på ett sätt som innebär att personuppgifterna inte längre kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används, under förutsättning att dessa kompletterande uppgifter förvaras separat och är föremål för tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna inte tillskrivs en identifierad eller identifierbar fysisk person,

6. *register*: en strukturerad samling av personuppgifter som är tillgänglig enligt särskilda kriterier, oavsett om samlingen är centraliserad, decentraliserad eller spridd på grundval av funktionella eller geografiska förhållanden,

7. *personuppgiftsansvarig*: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter; om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt,

8. *personuppgiftsbiträde*: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning,

9. *mottagare*: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ till vilket personuppgifterna utlämnas, vare sig det är en tredje part eller inte; offentliga myndigheter som kan komma att motta

personuppgifter inom ramen för ett särskilt uppdrag i enlighet med unionsrätten eller medlemsstaternas nationella rätt ska dock inte betraktas som mottagare; offentliga myndigheters behandling av dessa uppgifter ska vara förenlig med tillämpliga bestämmelser för dataskydd beroende på behandlingens syfte,

10. *tredje part*: en fysisk eller juridisk person, offentlig myndighet, institution eller organ som inte är den registrerade, den personuppgiftsansvarige, personuppgiftsbiträdet eller de personer som under den personuppgiftsansvariges eller personuppgiftsbiträdets direkta ansvar är behöriga att behandla personuppgifterna,

11. *samtycke* av den registrerade: varje slag av frivillig, specifik, informerad och otvetydig viljeyttring, genom vilken den registrerade, antingen genom ett uttalande eller genom en entydig bekräftande handling, godtar behandling av personuppgifter som rör honom eller henne,

12. *personuppgiftsincident*: en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats,

13. *genetiska uppgifter*: alla personuppgifter som rör nedärvda eller förvärvade genetiska kännetecken för en fysisk person, vilka ger unik information om denna fysiska persons fysiologi eller hälsa och vilka framför allt härrör från en analys av ett biologiskt prov från den fysiska personen i fråga,

14. *biometriska uppgifter*: personuppgifter som erhållits genom en särskild teknisk behandling som rör en fysisk persons fysiska, fysiologiska eller beteendemässiga kännetecken och som möjliggör eller bekräftar identifieringen av denna fysiska person, såsom ansiktsbilder eller fingeravtrycksuppgifter,

15. *uppgifter om hälsa*: personuppgifter som rör en fysisk persons fysiska eller psykiska hälsa, inbegripet tillhandahållande av hälso- och sjukvårdstjänster, vilka ger information om dennes hälsostatus,

16. *huvudsakligt verksamhetsställe*:

    a) när det gäller en personuppgiftsansvarig med verksamhetsställen i mer än en medlemsstat, den plats i unionen där vederbörande har sin centrala förvaltning, om inte besluten om ändamålen och medlen för behandlingen av personuppgifter fattas vid ett annat av den personuppgiftsansvariges verksamhetsställen i unionen och det sistnämnda verksamhetsstället har befogenhet att få sådana beslut genomförda, i vilket fall det verksamhetsställe som har fattat sådana beslut ska betraktas som det huvudsakliga verksamhetsstället,

    b) när det gäller ett personuppgiftsbiträde med verksamhetsställen i mer än en medlemsstat, den plats i unionen där vederbörande har sin centrala förvaltning eller, om personuppgiftsbiträdet inte har någon central förvaltning i unionen, det av personuppgiftsbiträdets verksamhetsställen i unionen där den huvudsakliga behandlingen inom ramen för verksamheten vid ett av personuppgiftsbiträdets verksamhetsställen sker, i den utsträckning som personuppgiftsbiträdet omfattas av särskilda skyldigheter enligt denna förordning,

17. *företrädare*: en i unionen etablerad fysisk eller juridisk person som skriftligen har utsetts av den personuppgiftsansvarige eller personuppgiftsbiträdet i enlighet med artikel 27 och företräder denne i frågor som gäller dennes skyldigheter enligt denna förordning,

18. *företag*: en fysisk eller juridisk person som bedriver ekonomisk verksamhet, oavsett dess juridiska form, vilket inbegriper partnerskap eller föreningar som regelbundet bedriver ekonomisk verksamhet,

19. *koncern*: ett kontrollerande företag och dess kontrollerade företag,

20. *bindande företagsbestämmelser*: strategier för skydd av personuppgifter som en personuppgiftsansvarig eller ett personuppgiftsbiträde som är etablerad på en medlemsstats territorium använder sig av vid överföringar eller en uppsättning av överföringar av personuppgifter till en personuppgiftsansvarig eller ett personuppgiftsbiträde i ett eller flera tredjeländer inom en koncern eller en grupp av företag som deltar i gemensam ekonomisk verksamhet,

21. *tillsynsmyndighet*: en oberoende offentlig myndighet som är utsedd av en medlemsstat i enlighet med artikel 51,

22. *berörd tillsynsmyndighet*: en tillsynsmyndighet som berörs av behandlingen av personuppgifter på grund av att

a) den personuppgiftsansvarige eller personuppgiftsbiträdet är etablerad på tillsynsmyndighetens medlemsstats territorium,

b) registrerade som är bosatta i den tillsynsmyndighetens medlemsstat i väsentlig grad påverkas eller sannolikt i väsentlig grad kommer att påverkas av behandlingen, eller

c) ett klagomål har lämnats in till denna tillsynsmyndighet,

23. *gränsöverskridande behandling*:

a) behandling av personuppgifter som äger rum inom ramen för verksamhet vid verksamhetsställen i mer än en medlemsstat tillhörande en personuppgiftsansvarig eller ett personuppgiftsbiträde i unionen, när den personuppgiftsansvarige eller personuppgiftsbiträdet är etablerad i mer än en medlemsstat, eller

b) behandling av personuppgifter som äger rum inom ramen för verksamhet vid ett enda verksamhetsställe tillhörande en personuppgiftsansvarig eller ett personuppgiftsbiträde i unionen men som i väsentlig grad påverkar eller sannolikt i väsentlig grad kommer att påverka registrerade i mer än en medlemsstat,

24. *relevant och motiverad invändning*: en invändning mot ett förslag till beslut avseende frågan huruvida det föreligger en överträdelse av denna förordning eller huruvida den planerade åtgärden i förhållande till den personuppgiftsansvarige eller personuppgiftsbiträdet är förenlig med denna förordning, av vilken invändning det tydligt framgår hur stora risker utkastet till beslut medför när det gäller registrerades grundläggande rättigheter och friheter samt i tillämpliga fall det fria flödet av personuppgifter inom unionen,

25. *informationssamhällets tjänster*: alla tjänster enligt definitionen i artikel 1.1 b i Europaparlamentets och rådets direktiv (EU) 2015/1535 ([1]),

26. *internationell organisation*: en organisation och dess underställda organ som lyder under folkrätten, eller ett annat organ som inrättats genom eller på grundval av en överenskommelse mellan två eller flera länder.

KAPITEL II

Principer

Artikel 5

Principer för behandling av personuppgifter

1. Vid behandling av personuppgifter ska följande gälla:

a) Uppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade (*laglighet, korrekthet och öppenhet*).

b) De ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål. Ytterligare behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1 ska inte anses vara oförenlig med de ursprungliga ändamålen (*ändamålsbegränsning*).

c) De ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas (*uppgiftsminimering*).

d) De ska vara korrekta och om nödvändigt uppdaterade. 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 (*korrekthet*).

([1]) Europaparlamentets och rådets direktiv (EU) 2015/1535 av den 9 september 2015 om ett informationsförfarande beträffande tekniska föreskrifter och beträffande föreskrifter för informationssamhällets tjänster (EUT L 241, 17.9.2015, s. 1).

e) De får inte förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas. Personuppgifter får lagras under längre perioder i den mån som personuppgifterna enbart behandlas för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1, under förutsättning att de lämpliga tekniska och organisatoriska åtgärder som krävs enligt denna förordning genomförs för att säkerställa den registrerades rättigheter och friheter (*lagringsminimering*).

f) De ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder (*integritet och konfidentialitet*).

2. Den personuppgiftsansvarige ska ansvara för och kunna visa att punkt 1 efterlevs (*ansvarsskyldighet*).

Artikel 6

Laglig behandling av personuppgifter

1. Behandling är endast laglig om och i den mån som åtminstone ett av följande villkor är uppfyllt:

a) Den registrerade har lämnat sitt samtycke till att dennes personuppgifter behandlas för ett eller flera specifika ändamål.

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.

c) Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige.

d) Behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person.

e) Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.

f) Behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter, särskilt när den registrerade är ett barn.

Led f i första stycket ska inte gälla för behandling som utförs av offentliga myndigheter när de fullgör sina uppgifter.

2. Medlemsstaterna får behålla eller införa mer specifika bestämmelser för att anpassa tillämpningen av bestämmelserna i denna förordning med hänsyn till behandling för att efterleva punkt 1 c och e genom att närmare fastställa specifika krav för uppgiftsbehandlingen och andra åtgärder för att säkerställa en laglig och rättvis behandling, inbegripet för andra specifika situationer då uppgifter behandlas i enlighet med kapitel IX.

3. Den grund för behandlingen som avses i punkt 1 c och e ska fastställas i enlighet med

a) unionsrätten, eller

b) en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av.

Syftet med behandlingen ska fastställas i den rättsliga grunden eller, i fråga om behandling enligt punkt 1 e, ska vara nödvändigt för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning. Den rättsliga grunden kan innehålla särskilda bestämmelser för att anpassa tillämpningen av bestämmelserna i denna förordning, bland annat: de allmänna villkor som ska gälla för den personuppgiftsansvariges behandling, vilken typ av uppgifter som ska behandlas, vilka registrerade som berörs, de enheter till vilka personuppgifterna får lämnas ut och för vilka ändamål, ändamålsbegränsningar, lagringstid samt typer av behandling och förfaranden för behandling, inbegripet åtgärder för att tillförsäkra en laglig och rättvis behandling, däribland för behandling i andra särskilda

situationer enligt kapitel IX. Unionsrätten eller medlemsstaternas nationella rätt ska uppfylla ett mål av allmänt intresse och vara proportionell mot det legitima mål som eftersträvas.

4. Om en behandling för andra ändamål än det ändamål för vilket personuppgifterna samlades in inte grundar sig på den registrerades samtycke eller på unionsrätten eller medlemsstaternas nationella rätt som utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle för att skydda de mål som avses i artikel 23.1, ska den personuppgiftsansvarige för att fastställa huruvida behandling för andra ändamål är förenlig med det ändamål för vilket personuppgifterna ursprungligen samlades in bland annat beakta följande:

a) Kopplingar mellan de ändamål för vilka personuppgifterna har samlats in och ändamålen med den avsedda ytterligare behandlingen.

b) Det sammanhang inom vilket personuppgifterna har samlats in, särskilt förhållandet mellan de registrerade och den personuppgiftsansvarige.

c) Personuppgifternas art, särskilt huruvida särskilda kategorier av personuppgifter behandlas i enlighet med artikel 9 eller huruvida personuppgifter om fällande domar i brottmål och överträdelser behandlas i enlighet med artikel 10.

d) Eventuella konsekvenser för registrerade av den planerade fortsatta behandlingen.

e) Förekomsten av lämpliga skyddsåtgärder, vilket kan inbegripa kryptering eller pseudonymisering.

Artikel 7

Villkor för samtycke

1. Om behandlingen grundar sig på samtycke, ska den personuppgiftsansvarige kunna visa att den registrerade har samtyckt till behandling av sina personuppgifter.

2. Om den registrerades samtycke lämnas i en skriftlig förklaring som också rör andra frågor, ska begäran om samtycke läggas fram på ett sätt som klart och tydligt kan särskiljas från de andra frågorna i en begriplig och lätt tillgänglig form, med användning av klart och tydligt språk. Om en del av förklaringen innebär en överträdelse av denna förordning, ska denna del inte vara bindande.

3. De registrerade ska ha rätt att när som helst återkalla sitt samtycke. Återkallandet av samtycket ska inte påverka lagligheten av behandling som grundar sig på samtycke, innan detta återkallas. Innan samtycke lämnas ska den registrerade informeras om detta. Det ska vara lika lätt att återkalla som att ge sitt samtycke.

4. Vid bedömning av huruvida samtycke är frivilligt ska största hänsyn bland annat tas till huruvida genomförandet av ett avtal, inbegripet tillhandahållandet av en tjänst, har gjorts beroende av samtycke till sådan behandling av personuppgifter som inte är nödvändig för genomförandet av det avtalet.

Artikel 8

Villkor som gäller barns samtycke avseende informationssamhällets tjänster

1. Vid erbjudande av informationssamhällets tjänster direkt till ett barn, ska vid tillämpningen av artikel 6.1 a behandling av personuppgifter som rör ett barn vara tillåten om barnet är minst 16 år. Om barnet är under 16 år ska sådan behandling vara tillåten endast om och i den mån samtycke ges eller godkänns av den person som har föräldraansvar för barnet.

Medlemsstaterna får i sin nationella rätt föreskriva en lägre ålder i detta syfte, under förutsättning att denna lägre ålder inte är under 13 år.

2. Den personuppgiftsansvarige ska göra rimliga ansträngningar för att i sådana fall kontrollera att samtycke ges eller godkänns av den person som har föräldraansvar för barnet, med hänsyn tagen till tillgänglig teknik.

3. Punkt 1 ska inte påverka tillämpningen av allmän avtalsrätt i medlemsstaterna, såsom bestämmelser om giltigheten, upprättandet eller effekten av ett avtal som gäller ett barn.

Artikel 9

Behandling av särskilda kategorier av personuppgifter

1. Behandling av personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning ska vara förbjuden.

2. Punkt 1 ska inte tillämpas om något av följande gäller:

a) Den registrerade har uttryckligen lämnat sitt samtycke till behandlingen av dessa personuppgifter för ett eller flera specifika ändamål, utom då unionsrätten eller medlemsstaternas nationella rätt föreskriver att förbudet i punkt 1 inte kan upphävas av den registrerade.

b) Behandlingen är nödvändig för att den personuppgiftsansvarige eller den registrerade ska kunna fullgöra sina skyldigheter och utöva sina särskilda rättigheter inom arbetsrätten och på områdena social trygghet och socialt skydd, i den omfattning detta är tillåtet enligt unionsrätten eller medlemsstaternas nationella rätt eller ett kollektivavtal som antagits med stöd av medlemsstaternas nationella rätt, där lämpliga skyddsåtgärder som säkerställer den registrerades grundläggande rättigheter och intressen fastställs.

c) Behandlingen är nödvändig för att skydda den registrerades eller någon annan fysisk persons grundläggande intressen när den registrerade är fysiskt eller rättsligt förhindrad att ge sitt samtycke.

d) Behandlingen utförs inom ramen för berättigad verksamhet med lämpliga skyddsåtgärder hos en stiftelse, en förening eller ett annat icke vinstdrivande organ, som har ett politiskt, filosofiskt, religiöst eller fackligt syfte, förutsatt att behandlingen enbart rör sådana organs medlemmar eller tidigare medlemmar eller personer som på grund av organets ändamål har regelbunden kontakt med detta och personuppgifterna inte lämnas ut utanför det organet utan den registrerades samtycke.

e) Behandlingen rör personuppgifter som på ett tydligt sätt har offentliggjorts av den registrerade.

f) Behandlingen är nödvändig för att fastställa, göra gällande eller försvara rättsliga anspråk eller som en del av domstolarnas dömande verksamhet.

g) Behandlingen är nödvändig av hänsyn till ett viktigt allmänt intresse, på grundval av unionsrätten eller medlemsstaternas nationella rätt, vilken ska stå i proportion till det eftersträvade syftet, vara förenligt med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.

h) Behandlingen är nödvändig av skäl som hör samman med förebyggande hälso- och sjukvård och yrkesmedicin, bedömningen av en arbetstagares arbetskapacitet, medicinska diagnoser, tillhandahållande av hälso- och sjukvård, behandling, social omsorg eller förvaltning av hälso- och sjukvårdstjänster och social omsorg och av deras system, på grundval av unionsrätten eller medlemsstaternas nationella rätt eller enligt avtal med yrkesverksamma på hälsoområdet och under förutsättning att de villkor och skyddsåtgärder som avses i punkt 3 är uppfyllda.

i) Behandlingen är nödvändig av skäl av allmänt intresse på folkhälsoområdet, såsom behovet av att säkerställa ett skydd mot allvarliga gränsöverskridande hot mot hälsan eller säkerställa höga kvalitets- och säkerhetsnormer för vård och läkemedel eller medicintekniska produkter, på grundval av unionsrätten eller medlemsstaternas nationella rätt, där lämpliga och specifika åtgärder för att skydda den registrerades rättigheter och friheter fastställs, särskilt tystnadsplikt.

j) Behandlingen är nödvändig för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1, på grundval av unionsrätten eller medlemsstaternas nationella rätt, vilken ska stå i proportion till det eftersträvade syftet, vara förenligt med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.

3. Personuppgifter som avses i punkt 1 får behandlas för de ändamål som avses i punkt 2 h, när uppgifterna behandlas av eller under ansvar av en yrkesutövare som omfattas av tystnadsplikt enligt unionsrätten eller medlemsstaternas nationella rätt eller bestämmelser som fastställs av nationella behöriga organ eller av en annan person som också omfattas av tystnadsplikt enligt unionsrätten eller medlemsstaternas nationella rätt eller bestämmelser som fastställs av nationella behöriga organ.

4. Medlemsstaterna får behålla eller införa ytterligare villkor, även begränsningar, för behandlingen av genetiska eller biometriska uppgifter eller uppgifter om hälsa.

Artikel 10

Behandling av personuppgifter som rör fällande domar i brottmål samt överträdelser

Behandling av personuppgifter som rör fällande domar i brottmål och överträdelser eller därmed sammanhängande säkerhetsåtgärder enligt artikel 6.1 får endast utföras under kontroll av myndighet eller då behandling är tillåten enligt unionsrätten eller medlemsstaternas nationella rätt, där lämpliga skyddsåtgärder för de registrerades rättigheter och friheter fastställs. Ett fullständigt register över fällande domar i brottmål får endast föras under kontroll av en myndighet.

Artikel 11

Behandling som inte kräver identifiering

1. Om de ändamål för vilka den personuppgiftsansvarige behandlar personuppgifter inte kräver eller inte längre kräver att den registrerade identifieras av den personuppgiftsansvarige, ska den personuppgiftsansvarige inte vara tvungen att bevara, förvärva eller behandla ytterligare information för att identifiera den registrerade endast i syfte att följa denna förordning.

2. Om den personuppgiftsansvarige, i de fall som avses i punkt 1 i denna artikel, kan visa att denne inte är i stånd att identifiera den registrerade, ska den personuppgiftsansvarige om möjligt informera den registrerade om detta. I sådana fall ska artiklarna 15–20 inte gälla, förutom när den registrerade för utövande av sina rättigheter i enlighet med dessa artiklar tillhandahåller ytterligare information som gör identifieringen möjlig.

KAPITEL III

Den registrerades rättigheter

Avsnitt 1

Insyn och villkor

Artikel 12

Klar och tydlig information och kommunikation samt klara och tydliga villkor för utövandet av den registrerades rättigheter

1. Den personuppgiftsansvarige ska vidta lämpliga åtgärder för att till den registrerade tillhandahålla all information som avses i artiklarna 13 och 14 och all kommunikation enligt artiklarna 15–22 och 34 vilken avser behandling i en koncis, klar och tydlig, begriplig och lätt tillgänglig form, med användning av klart och tydligt språk, i synnerhet för information som är särskilt riktad till barn. Informationen ska tillhandahållas skriftligt, eller i någon annan form, inbegripet, när så är lämpligt, i elektronisk form. Om den registrerade begär det får informationen tillhandahållas muntligt, förutsatt att den registrerades identitet bevisats på andra sätt.

2. Den personuppgiftsansvarige ska underlätta utövandet av den registrerades rättigheter i enlighet med artiklarna 15–22. I de fall som avses i artikel 11.2 får den personuppgiftsansvarige inte vägra att tillmötesgå den registrerades begäran om att utöva sina rättigheter enligt artiklarna 15–22, om inte den personuppgiftsansvarige visar att han eller hon inte är i stånd att identifiera den registrerade.

3. Den personuppgiftsansvarige ska på begäran utan onödigt dröjsmål och under alla omständigheter senast en månad efter att ha mottagit begäran tillhandahålla den registrerade information om de åtgärder som vidtagits enligt artiklarna 15–22. Denna period får vid behov förlängas med ytterligare två månader, med beaktande av hur komplicerad begäran är och antalet inkomna begäranden. Den personuppgiftsansvarige ska underrätta den registrerade om en sådan förlängning inom en månad från det att begäran mottagits samt ange orsakerna till förseningen. Om den registrerade lämnar begäran i elektronisk form, ska informationen om möjligt tillhandahållas i elektronisk form, om den registrerade inte begär något annat.

4. Om den personuppgiftsansvarige inte vidtar åtgärder på den registrerades begäran, ska den personuppgiftsansvarige utan dröjsmål och senast en månad efter att ha mottagit begäran informera den registrerade om orsaken till att åtgärder inte vidtagits och om möjligheten att lämna in ett klagomål till en tillsynsmyndighet och begära rättslig prövning.

5. Information som tillhandahållits enligt artiklarna 13 och 14, all kommunikation och samtliga åtgärder som vidtas enligt artiklarna 15–22 och 34 ska tillhandahållas kostnadsfritt. Om begäranden från en registrerad är uppenbart ogrundade eller orimliga, särskilt på grund av deras repetitiva art, får den personuppgiftsansvarige antingen

a) ta ut en rimlig avgift som täcker de administrativa kostnaderna för att tillhandahålla den information eller vidta den åtgärd som begärts, eller

b) vägra att tillmötesgå begäran.

Det åligger den personuppgiftsansvarige att visa att begäran är uppenbart ogrundad eller orimlig.

6. Utan att det påverkar tillämpningen av artikel 11 får den personuppgiftsansvarige, om denne har rimliga skäl att betvivla identiteten hos den fysiska person som lämnar in en begäran enligt artiklarna 15–21, begära att ytterligare information som är nödvändig för att bekräfta den registrerades identitet tillhandahålls.

7. Den information som ska tillhandahållas de registrerade i enlighet med artiklarna 13 och 14 får tillhandahållas kombinerad med standardiserade symboler för att ge en överskådlig, begriplig, lättläst och meningsfull överblick över den planerade behandlingen. Om sådana symboler visas elektroniskt ska de vara maskinläsbara.

8. Kommissionen ska ges befogenhet att anta delegerade akter i enlighet med artikel 92 för att fastställa vilken information som ska visas med hjälp av symboler och förfaranden för att tillhandahålla sådana symboler.

Avsnitt 2

Information och tillgång till personuppgifter

Artikel 13

Information som ska tillhandahållas om personuppgifterna samlas in från den registrerade

1. Om personuppgifter som rör en registrerad person samlas in från den registrerade, ska den personuppgiftsansvarige, när personuppgifterna erhålls, till den registrerade lämna information om följande:

a) Identitet och kontaktuppgifter för den personuppgiftsansvarige och i tillämpliga fall för dennes företrädare.

b) Kontaktuppgifter för dataskyddsombudet, i tillämpliga fall.

c) Ändamålen med den behandling för vilken personuppgifterna är avsedda samt den rättsliga grunden för behandlingen.

d) Om behandlingen är baserad på artikel 6.1 f, den personuppgiftsansvariges eller en tredje parts berättigade intressen.

e) Mottagarna eller de kategorier av mottagare som ska ta del av personuppgifterna, i förekommande fall.

f) I tillämpliga fall att den personuppgiftsansvarige avser att överföra personuppgifter till ett tredjeland eller en internationell organisation och huruvida ett beslut av kommissionen om adekvat skyddsnivå föreligger eller saknas eller, när det gäller de överföringar som avses i artikel 46, 47 eller artikel 49.1 andra stycket, hänvisning till lämpliga eller passande skyddsåtgärder och hur en kopia av dem kan erhållas eller var dessa har gjorts tillgängliga.

2. Utöver den information som avses i punkt 1 ska den personuppgiftsansvarige vid insamlingen av personuppgifterna lämna den registrerade följande ytterligare information, vilken krävs för att säkerställa rättvis och transparent behandling:

a) Den period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period.

b) Att det föreligger en rätt att av den personuppgiftsansvarige begära tillgång till och rättelse eller radering av personuppgifter eller begränsning av behandling som rör den registrerade eller att invända mot behandling samt rätten till dataportabilitet.

c) Om behandlingen grundar sig på artikel 6.1 a eller artikel 9.2 a, att det föreligger en rätt att när som helst återkalla sitt samtycke, utan att detta påverkar lagligheten av behandlingen på grundval av samtycket, innan detta återkallades.

d) Rätten att inge klagomål till en tillsynsmyndighet.

e) Huruvida tillhandahållandet av personuppgifter är ett lagstadgat eller avtalsenligt krav eller ett krav som är nödvändigt för att ingå ett avtal samt huruvida den registrerade är skyldig att tillhandahålla personuppgifterna och de möjliga följderna av att sådana uppgifter inte lämnas.

f) Förekomsten av automatiserat beslutsfattande, inbegripet profilering enligt artikel 22.1 och 22.4, varvid det åtminstone i dessa fall ska lämnas meningsfull information om logiken bakom samt betydelsen och de förutsedda följderna av sådan behandling för den registrerade.

3. Om den personuppgiftsansvarige avser att ytterligare behandla personuppgifterna för ett annat syfte än det för vilket de insamlades, ska den personuppgiftsansvarige före denna ytterligare behandling ge den registrerade information om detta andra syfte samt ytterligare relevant information enligt punkt 2.

4. Punkterna 1, 2 och 3 ska inte tillämpas om och i den mån den registrerade redan förfogar över informationen.

Artikel 14

Information som ska tillhandahållas om personuppgifterna inte har erhållits från den registrerade

1. Om personuppgifterna inte har erhållits från den registrerade, ska den personuppgiftsansvarige förse den registrerade med följande information:

a) Identitet och kontaktuppgifter för den personuppgiftsansvarige och i tillämpliga fall för dennes företrädare.

b) Kontaktuppgifter för dataskyddsombudet, i tillämpliga fall.

c) Ändamålen med den behandling för vilken personuppgifterna är avsedda samt den rättsliga grunden för behandlingen.

d) De kategorier av personuppgifter som behandlingen gäller.

e) Mottagarna eller de kategorier av mottagare som ska ta del av personuppgifterna, i förekommande fall.

f) I tillämpliga fall att den personuppgiftsansvarige avser att överföra personuppgifter till en mottagare i ett tredjeland eller en internationell organisation och huruvida ett beslut av kommissionen om adekvat skyddsnivå föreligger eller saknas eller, när det gäller de överföringar som avses i artiklarna 46, 47 eller artikel 49.1 andra stycket, hänvisning till lämpliga eller passande skyddsåtgärder och hur en kopia av dem kan erhållas eller var dessa har gjorts tillgängliga.

2. Utöver den information som avses i punkt 1 ska den personuppgiftsansvarige lämna den registrerade följande information, vilken krävs för att säkerställa rättvis och transparent behandling när det gäller den registrerade:

a) Den period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period.

b) Om behandlingen grundar sig på artikel 6.1 f, den personuppgiftsansvariges eller en tredje parts berättigade intressen.

c) Förekomsten av rätten att av den personuppgiftsansvarige begära tillgång till och rättelse eller radering av personuppgifter eller begränsning av behandling som rör den registrerade och att invända mot behandling samt rätten till dataportabilitet.

d) Om behandlingen grundar sig på artikel 6.1 a eller artikel 9.2 a, rätten att när som helst återkalla sitt samtycke, utan att detta påverkar lagligheten av behandlingen på grundval av samtycket, innan detta återkallades.

e) Rätten att inge klagomål till en tillsynsmyndighet.

f) Varifrån personuppgifterna kommer och i förekommande fall huruvida de har sitt ursprung i allmänt tillgängliga källor.

g) Förekomsten av automatiserat beslutsfattande, inbegripet profilering enligt artikel 22.1 och 22.4, varvid det åtminstone i dessa fall ska lämnas meningsfull information om logiken bakom samt betydelsen och de förutsedda följderna av sådan behandling för den registrerade.

3. Den personuppgiftsansvarige ska lämna den information som anges i punkterna 1 och 2

a) inom en rimlig period efter det att personuppgifterna har erhållits, dock senast inom en månad, med beaktande av de särskilda omständigheter under vilka personuppgifterna behandlas,

b) om personuppgifterna ska användas för kommunikation med den registrerade, senast vid tidpunkten för den första kommunikationen med den registrerade, eller

c) om ett utlämnande till en annan mottagare förutses, senast när personuppgifterna lämnas ut för första gången.

4. Om den personuppgiftsansvarige avser att ytterligare behandla personuppgifterna för ett annat syfte än det för vilket de insamlades, ska den personuppgiftsansvarige före denna ytterligare behandling ge den registrerade information om detta andra syfte samt ytterligare relevant information enligt punkt 2.

5. Punkterna 1–4 ska inte tillämpas i följande fall och i den mån

a) den registrerade redan förfogar över informationen,

b) tillhandahållandet av sådan information visar sig vara omöjligt eller skulle medföra en oproportionell ansträngning, särskilt för behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1, eller i den mån den skyldighet som avses i punkt 1 i den här artikeln sannolikt kommer att göra det omöjligt eller avsevärt försvårar uppfyllandet av målen med den behandlingen; i sådana fall ska den personuppgiftsansvarige vidta lämpliga åtgärder för att skydda den registrerades rättigheter och friheter och berättigade intressen, inbegripet göra uppgifterna tillgängliga för allmänheten,

c) erhållande eller utlämnande av uppgifter uttryckligen föreskrivs genom unionsrätten eller genom en medlemsstats nationella rätt som den registrerade omfattas av och som fastställer lämpliga åtgärder för att skydda den registrerades berättigade intressen, eller

d) personuppgifterna måste förbli konfidentiella till följd av tystnadsplikt enligt unionsrätten eller medlemsstaternas nationella rätt, inbegripet andra lagstadgade sekretessförpliktelser.

Artikel 15

Den registrerades rätt till tillgång

1. Den registrerade ska ha rätt att av den personuppgiftsansvarige få bekräftelse på huruvida personuppgifter som rör honom eller henne håller på att behandlas och i så fall få tillgång till personuppgifterna och följande information:

a) Ändamålen med behandlingen.

b) De kategorier av personuppgifter som behandlingen gäller.

c) De mottagare eller kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut, särskilt mottagare i tredjeländer eller internationella organisationer.

d) Om möjligt, den förutsedda period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period.

e) Förekomsten av rätten att av den personuppgiftsansvarige begära rättelse eller radering av personuppgifterna eller begränsningar av behandling av personuppgifter som rör den registrerade eller att invända mot sådan behandling.

f) Rätten att inge klagomål till en tillsynsmyndighet.

g) Om personuppgifterna inte samlas in från den registrerade, all tillgänglig information om varifrån dessa uppgifter kommer.

h) Förekomsten av automatiserat beslutsfattande, inbegripet profilering enligt artikel 22.1 och 22.4, varvid det åtminstone i dessa fall ska lämnas meningsfull information om logiken bakom samt betydelsen och de förutsedda följderna av sådan behandling för den registrerade.

2. Om personuppgifterna överförs till ett tredjeland eller till en internationell organisation, ska den registrerade ha rätt till information om de lämpliga skyddsåtgärder som i enlighet med artikel 46 har vidtagits vid överföringen.

3. Den personuppgiftsansvarige ska förse den registrerade med en kopia av de personuppgifter som är under behandling. För eventuella ytterligare kopior som den registrerade begär får den personuppgiftsansvarige ta ut en rimlig avgift på grundval av de administrativa kostnaderna. Om den registrerade gör begäran i elektronisk form ska informationen tillhandahållas i ett elektroniskt format som är allmänt använt, om den registrerade inte begär något annat.

4. Den rätt till en kopia som avses i punkt 3 ska inte inverka menligt på andras rättigheter och friheter.

Avsnitt 3

Rättelse och radering

Artikel 16

Rätt till rättelse

Den registrerade ska ha rätt att av den personuppgiftsansvarige utan onödigt dröjsmål få felaktiga personuppgifter som rör honom eller henne rättade. Med beaktande av ändamålet med behandlingen, ska den registrerade ha rätt att komplettera ofullständiga personuppgifter, bland annat genom att tillhandahålla ett kompletterande utlåtande.

Artikel 17

Rätt till radering (”rätten att bli bortglömd”)

1. Den registrerade ska ha rätt att av den personuppgiftsansvarige utan onödigt dröjsmål få sina personuppgifter raderade och den personuppgiftsansvarige ska vara skyldig att utan onödigt dröjsmål radera personuppgifter om något av följande gäller:

a) Personuppgifterna är inte längre nödvändiga för de ändamål för vilka de samlats in eller på annat sätt behandlats.

b) Den registrerade återkallar det samtycke på vilket behandlingen grundar sig enligt artikel 6.1 a eller artikel 9.2 a och det finns inte någon annan rättslig grund för behandlingen.

c) Den registrerade invänder mot behandlingen i enlighet med artikel 21.1 och det saknas berättigade skäl för behandlingen som väger tyngre, eller den registrerade invänder mot behandlingen i enlighet med artikel 21.2.

d) Personuppgifterna har behandlats på olagligt sätt.

e) Personuppgifterna måste raderas för att uppfylla en rättslig förpliktelse i unionsrätten eller i medlemsstaternas nationella rätt som den personuppgiftsansvarige omfattas av.

f) Personuppgifterna har samlats in i samband med erbjudande av informationssamhällets tjänster, i de fall som avses i artikel 8.1.

2. Om den personuppgiftsansvarige har offentliggjort personuppgifterna och enligt punkt 1 är skyldig att radera personuppgifterna, ska den personuppgiftsansvarige med beaktande av tillgänglig teknik och kostnaden för genomförandet vidta rimliga åtgärder, inbegripet tekniska åtgärder, för att underrätta personuppgiftsansvariga som behandlar personuppgifterna om att den registrerade har begärt att de ska radera eventuella länkar till, eller kopior eller reproduktioner av dessa personuppgifter.

3. Punkterna 1 och 2 ska inte gälla i den utsträckning som behandlingen är nödvändig av följande skäl:

a) För att utöva rätten till yttrande- och informationsfrihet.

b) För att uppfylla en rättslig förpliktelse som kräver behandling enligt unionsrätten eller enligt en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av eller för att utföra en uppgift av allmänt intresse eller som är ett led i myndighetsutövning som utförs av den personuppgiftsansvarige.

c) För skäl som rör ett viktigt allmänt intresse på folkhälsoområdet enligt artikel 9.2 h och i samt artikel 9.3.

d) För arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål enligt artikel 89.1, i den utsträckning som den rätt som avses i punkt 1 sannolikt omöjliggör eller avsevärt försvårar uppnåendet av syftet med den behandlingen.

e) För att kunna fastställa, göra gällande eller försvara rättsliga anspråk.

Artikel 18

Rätt till begränsning av behandling

1. Den registrerade ska ha rätt att av den personuppgiftsansvarige kräva att behandlingen begränsas om något av följande alternativ är tillämpligt:

a) Den registrerade bestrider personuppgifternas korrekthet, under en tid som ger den personuppgiftsansvarige möjlighet att kontrollera om personuppgifterna är korrekta.

b) Behandlingen är olaglig och den registrerade motsätter sig att personuppgifterna raderas och i stället begär en begränsning av deras användning.

c) Den personuppgiftsansvarige behöver inte längre personuppgifterna för ändamålen med behandlingen men den registrerade behöver dem för att kunna fastställa, göra gällande eller försvara rättsliga anspråk.

d) Den registrerade har invänt mot behandling i enlighet med artikel 21.1 i väntan på kontroll av huruvida den personuppgiftsansvariges berättigade skäl väger tyngre än den registrerades berättigade skäl.

2. Om behandlingen har begränsats i enlighet med punkt 1 får sådana personuppgifter, med undantag för lagring, endast behandlas med den registrerades samtycke eller för att fastställa, göra gällande eller försvara rättsliga anspråk eller för att skydda någon annan fysisk eller juridisk persons rättigheter eller för skäl som rör ett viktigt allmänintresse för unionen eller för en medlemsstat.

3. En registrerad som har fått behandling begränsad i enlighet med punkt 1 ska underrättas av den personuppgiftsansvarige innan begränsningen av behandlingen upphör.

Artikel 19

Anmälningsskyldighet avseende rättelse eller radering av personuppgifter och begränsning av behandling

Den personuppgiftsansvarige ska underrätta varje mottagare till vilken personuppgifterna har lämnats ut om eventuella rättelser eller radering av personuppgifter eller begränsningar av behandling som skett i enlighet med artiklarna 16, 17.1 och 18, om inte detta visar sig vara omöjligt eller medföra en oproportionell ansträngning. Den personuppgiftsansvarige ska informera den registrerade om dessa mottagare på den registrerades begäran.

Artikel 20

Rätt till dataportabilitet

1. Den registrerade ska ha rätt att få ut de personuppgifter som rör honom eller henne och som han eller hon har tillhandahållit den personuppgiftsansvarige i ett strukturerat, allmänt använt och maskinläsbart format och ha rätt att överföra dessa uppgifter till en annan personuppgiftsansvarig utan att den personuppgiftsansvarige som tillhandahållits personuppgifterna hindrar detta, om

a) behandlingen grundar sig på samtycke enligt artikel 6.1 a eller artikel 9.2 a eller på ett avtal enligt artikel 6.1 b, och

b) behandlingen sker automatiserat.

2 Vid utövandet av sin rätt till dataportabilitet i enlighet med punkt 1 ska den registrerade ha rätt till överföring av personuppgifterna direkt från en personuppgiftsansvarig till en annan, när detta är tekniskt möjligt.

3. Utövandet av den rätt som avses i punkt 1 i den här artikeln ska inte påverka tillämpningen av artikel 17. Den rätten ska inte gälla i fråga om en behandling som är nödvändig för att utföra en uppgift av allmänt intresse eller som är ett led i myndighetsutövning som utförs av den personuppgiftsansvarige.

4. Den rätt som avses i punkt 1 får inte påverka andras rättigheter och friheter på ett ogynnsamt sätt.

Avsnitt 4

Rätt att göra invändningar och automatiserat individuellt beslutsfattande

Artikel 21

Rätt att göra invändningar

1. Den registrerade ska, av skäl som hänför sig till hans eller hennes specifika situation, ha rätt att när som helst göra invändningar mot behandling av personuppgifter avseende honom eller henne som grundar sig på artikel 6.1 e eller f, inbegripet profilering som grundar sig på dessa bestämmelser. Den personuppgiftsansvarige får inte längre behandla personuppgifterna såvida denne inte kan påvisa tvingande berättigade skäl för behandlingen som väger tyngre än den registrerades intressen, rättigheter och friheter eller om det sker för fastställande, utövande eller försvar av rättsliga anspråk.

2. Om personuppgifterna behandlas för direkt marknadsföring ska den registrerade ha rätt att när som helst invända mot behandling av personuppgifter som avser honom eller henne för sådan marknadsföring, vilket inkluderar profilering i den utsträckning som denna har ett samband med sådan direkt marknadsföring.

3. Om den registrerade invänder mot behandling för direkt marknadsföring ska personuppgifterna inte längre behandlas för sådana ändamål.

4. Senast vid den första kommunikationen med den registrerade ska den rätt som avses i punkterna 1 och 2 uttryckligen meddelas den registrerade och redovisas tydligt, klart och åtskilt från eventuell annan information.

5. När det gäller användningen av informationssamhällets tjänster, och trots vad som sägs i direktiv 2002/58/EG, får den registrerade utöva sin rätt att göra invändningar på automatiserat sätt med användning av tekniska specifikationer.

6. Om personuppgifter behandlas för vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1 ska den registrerade, av skäl som hänför sig till hans eller hennes specifika situation, ha rätt att göra invändningar mot behandling av personuppgifter avseende honom eller henne om inte behandlingen är nödvändig för att utföra en uppgift av allmänt intresse.

Artikel 22

Automatiserat individuellt beslutsfattande, inbegripet profilering

1. Den registrerade ska ha rätt att inte bli föremål för ett beslut som enbart grundas på automatiserad behandling, inbegripet profilering, vilket har rättsliga följder för honom eller henne eller på liknande sätt i betydande grad påverkar honom eller henne.

2. Punkt 1 ska inte tillämpas om beslutet

a) är nödvändigt för ingående eller fullgörande av ett avtal mellan den registrerade och den personuppgiftsansvarige,

b) tillåts enligt unionsrätten eller en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av och som fastställer lämpliga åtgärder till skydd för den registrerades rättigheter, friheter och berättigade intressen, eller

c) grundar sig på den registrerades uttryckliga samtycke.

3. I fall som avses i punkt 2 a och c ska den personuppgiftsansvarige genomföra lämpliga åtgärder för att säkerställa den registrerades rättigheter, friheter och rättsliga intressen, åtminstone rätten till personlig kontakt med den personuppgiftsansvarige för att kunna utrycka sin åsikt och bestrida beslutet.

4. Beslut enligt punkt 2 får inte grunda sig på de särskilda kategorier av personuppgifter som avses i artikel 9.1, såvida inte artikel 9.2 a eller g gäller och lämpliga åtgärder som ska skydda den registrerades berättigade intressen har vidtagits.

Avsnitt 5

Begränsningar

Artikel 23

Begränsningar

1. Det ska vara möjligt att i unionsrätten eller i en medlemsstats nationella rätt som den personuppgiftsansvarige eller personuppgiftsbiträdet omfattas av införa en lagstiftningsåtgärd som begränsar tillämpningsområdet för de skyldigheter och rättigheter som föreskrivs i artiklarna 12–22 och 34, samt artikel 5 i den mån dess bestämmelser motsvarar de rättigheter och skyldigheter som fastställs i artiklarna 12–22, om en sådan begränsning sker med respekt för andemeningen i de grundläggande rättigheterna och friheterna och utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle i syfte att säkerställa

a) den nationella säkerheten,

b) försvaret,

c) den allmänna säkerheten,

d) förebyggande, förhindrande, utredning, avslöjande eller lagföring av brott eller verkställande av straffrättsliga sanktioner, inbegripet skydd mot samt förebyggande och förhindrande av hot mot den allmänna säkerheten,

e) andra av unionens eller en medlemsstats viktiga mål av generellt allmänt intresse, särskilt ett av unionens eller en medlemsstats viktiga ekonomiska eller finansiella intressen, däribland penning-, budget- eller skattefrågor, folkhälsa och social trygghet,

f) skydd av rättsväsendets oberoende och rättsliga åtgärder,

g) förebyggande, förhindrande, utredning, avslöjande och lagföring av överträdelser av etiska regler som gäller för lagreglerade yrken,

h) en tillsyns-, inspektions- eller regleringsfunktion som, även i enstaka fall, har samband med myndighetsutövning i fall som nämns i a–e och g,

i) skydd av den registrerade eller andras rättigheter och friheter,

j) verkställighet av civilrättsliga krav.

2. Framför allt ska alla lagstiftningsåtgärder som avses i punkt 1 innehålla specifika bestämmelser åtminstone, när så är relevant, avseende

a) ändamålen med behandlingen eller kategorierna av behandling,

b) kategorierna av personuppgifter,

c) omfattningen av de införda begränsningarna,

d) skyddsåtgärder för att förhindra missbruk eller olaglig tillgång eller överföring,

e) specificeringen av den personuppgiftsansvarige eller kategorierna av personuppgiftsansvariga,

f) lagringstiden samt tillämpliga skyddsåtgärder med beaktande av behandlingens art, omfattning och ändamål eller kategorierna av behandling,

g) riskerna för de registrerades rättigheter och friheter, och

h) de registrerades rätt att bli informerade om begränsningen, såvida detta inte kan inverka menligt på begränsningen.

KAPITEL IV

Personuppgiftsansvarig och personuppgiftsbiträde

Avsnitt 1

Allmänna skyldigheter

Artikel 24

Den personuppgiftsansvariges ansvar

1. Med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med denna förordning. Dessa åtgärder ska ses över och uppdateras vid behov.

2. Om det står i proportion till behandlingen, ska de åtgärder som avses i punkt 1 omfatta den personuppgiftsansvariges genomförande av lämpliga strategier för dataskydd.

3. Tillämpningen av godkända uppförandekoder som avses i artikel 40 eller godkända certifieringsmekanismer som avses i artikel 42 får användas för att visa att den personuppgiftsansvarige fullgör sina skyldigheter.

Artikel 25

Inbyggt dataskydd och dataskydd som standard

1. Med beaktande av den senaste utvecklingen, genomförandekostnader och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige, både vid fastställandet av vilka medel behandlingen utförs med och vid själva behandlingen, genomföra lämpliga tekniska och organisatoriska åtgärder – såsom pseudonymisering – vilka är utformade för ett effektivt genomförande av dataskyddsprinciper – såsom uppgiftsminimering – och för integrering av de nödvändiga skyddsåtgärderna i behandlingen, så att kraven i denna förordning uppfylls och den registrerades rättigheter skyddas.

2. Den personuppgiftsansvarige ska genomföra lämpliga tekniska och organisatoriska åtgärder för att, i standardfallet, säkerställa att endast personuppgifter som är nödvändiga för varje specifikt ändamål med behandlingen behandlas. Den skyldigheten gäller mängden insamlade personuppgifter, behandlingens omfattning, tiden för deras lagring och deras tillgänglighet. Framför allt ska dessa åtgärder säkerställa att personuppgifter i standardfallet inte utan den enskildes medverkan görs tillgängliga för ett obegränsat antal fysiska personer.

3. En godkänd certifieringsmekanism i enlighet med artikel 42 får användas för att visa att kraven i punkterna 1 och 2 i den här artikeln följs.

Artikel 26

Gemensamt personuppgiftsansvariga

1. Om två eller fler personuppgiftsansvariga gemensamt fastställer ändamålen med och medlen för behandlingen ska de vara gemensamt personuppgiftsansvariga. Gemensamt personuppgiftsansvariga ska under öppna former fastställa sitt respektive ansvar för att fullgöra skyldigheterna enligt denna förordning, särskilt vad gäller utövandet av den registrerades rättigheter och sina respektive skyldigheter att tillhandahålla den information som avses i artiklarna 13 och 14, genom ett inbördes arrangemang, såvida inte de personuppgiftsansvarigas respektive skyldigheter fastställs genom unionsrätten eller en medlemsstats nationella rätt som de personuppgiftsansvariga omfattas av. Inom ramen för arrangemanget får en gemensam kontaktpunkt för de personuppgiftsansvariga utses.

2. Det arrangemang som avses i punkt 1 ska på lämpligt sätt återspegla de gemensamt personuppgiftsansvarigas respektive roller och förhållanden gentemot registrerade. Det väsentliga innehållet i arrangemanget ska göras tillgängligt för den registrerade.

3. Oavsett formerna för det arrangemang som avses i punkt 1 får den registrerade utöva sina rättigheter enligt denna förordning med avseende på och emot var och en av de personuppgiftsansvariga.

Artikel 27

Företrädare för personuppgiftsansvariga eller personuppgiftsbiträden som inte är etablerade i unionen

1. Om artikel 3.2 tillämpas ska den personuppgiftsansvarige eller personuppgiftsbiträdet skriftligen utse en företrädare i unionen.

2. Skyldigheten enligt punkt 1 i denna artikel ska inte gälla

a) tillfällig behandling som inte omfattar behandling i stor omfattning av särskilda kategorier av uppgifter, som avses i artikel 9.1, eller behandling av personuppgifter avseende fällande domar i brottmål samt överträdelser, som avses i artikel 10, och som sannolikt inte kommer att medföra en risk för fysiska personers rättigheter och friheter, med hänsyn till behandlingens art, sammanhang, omfattning och ändamål, eller

b) en offentlig myndighet eller ett offentligt organ.

3. Företrädaren ska vara etablerad i en av de medlemsstater där de registrerade, vars personuppgifter behandlas i samband med att de erbjuds varor eller tjänster, eller vars beteende övervakas, befinner sig.

4. Företrädaren ska på den personuppgiftsansvariges eller personuppgiftsbiträdets uppdrag, utöver eller i stället för den personuppgiftsansvarige eller personuppgiftsbiträdet, fungera som kontaktperson för i synnerhet tillsynsmyndigheter och registrerade, i alla frågor som har anknytning till behandlingen, i syfte att säkerställa efterlevnad av denna förordning.

5. Att den personuppgiftsansvarige eller personuppgiftsbiträdet utser en företrädare ska inte påverka de rättsliga åtgärder som skulle kunna inledas mot den personuppgiftsansvarige eller personuppgiftsbiträdet.

Artikel 28

Personuppgiftsbiträden

1. Om en behandling ska genomföras på en personuppgiftsansvarigs vägnar ska den personuppgiftsansvarige endast anlita personuppgiftsbiträden som ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i denna förordning och säkerställer att den registrerades rättigheter skyddas.

2. Personuppgiftsbiträdet får inte anlita ett annat personuppgiftsbiträde utan att ett särskilt eller allmänt skriftligt förhandstillstånd har erhållits av den personuppgiftsansvarige. Om ett allmänt skriftligt tillstånd har erhållits, ska personuppgiftsbiträdet informera den personuppgiftsansvarige om eventuella planer på att anlita nya personuppgiftsbiträden eller ersätta personuppgiftsbiträden, så att den personuppgiftsansvarige har möjlighet att göra invändningar mot sådana förändringar.

3. När uppgifter behandlas av ett personuppgiftsbiträde ska hanteringen regleras genom ett avtal eller en annan rättsakt enligt unionsrätten eller enligt medlemsstaternas nationella rätt som är bindande för personuppgiftsbiträdet med avseende på den personuppgiftsansvarige och i vilken föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade, samt den personuppgiftsansvariges skyldigheter och rättigheter anges. I det avtalet eller den rättsakten ska det särskilt föreskrivas att personuppgiftsbiträdet

a) endast får behandla personuppgifter på dokumenterade instruktioner från den personuppgiftsansvarige, inbegripet när det gäller överföringar av personuppgifter till ett tredjeland eller en internationell organisation, såvida inte denna behandling krävs enligt unionsrätten eller enligt en medlemsstats nationella rätt som personuppgiftsbiträdet omfattas av, och i så fall ska personuppgiftsbiträdet informera den personuppgiftsansvarige om det rättsliga kravet innan uppgifterna behandlas, såvida sådan information inte är förbjuden med hänvisning till ett viktigt allmänintresse enligt denna rätt,

b) säkerställer att personer med behörighet att behandla personuppgifterna har åtagit sig att iaktta konfidentialitet eller omfattas av en lämplig lagstadgad tystnadsplikt,

c) ska vidta alla åtgärder som krävs enligt artikel 32,

d) ska respektera de villkor som avses i punkterna 2 och 4 för anlitandet av ett annat personuppgiftsbiträde,

e) med tanke på behandlingens art, ska hjälpa den personuppgiftsansvarige genom lämpliga tekniska och organisatoriska åtgärder, i den mån detta är möjligt, så att den personuppgiftsansvarige kan fullgöra sin skyldighet att svara på begäran om utövande av den registrerades rättigheter i enlighet med kapitel III,

f) ska bistå den personuppgiftsansvarige med att se till att skyldigheterna enligt artiklarna 32–36 fullgörs, med beaktande av typen av behandling och den information som personuppgiftsbiträdet har att tillgå,

g) beroende på vad den personuppgiftsansvarige väljer, ska radera eller återlämna alla personuppgifter till den personuppgiftsansvarige efter det att tillhandahållandet av behandlingstjänster har avslutats, och radera befintliga kopior såvida inte lagring av personuppgifterna krävs enligt unionsrätten eller medlemsstaternas nationella rätt, och

h) ska ge den personuppgiftsansvarige tillgång till all information som krävs för att visa att de skyldigheter som fastställs i denna artikel har fullgjorts samt möjliggöra och bidra till granskningar, inbegripet inspektioner, som genomförs av den personuppgiftsansvarige eller av en annan revisor som bemyndigats av den personuppgiftsansvarige.

Med avseende på led h i första stycket ska personuppgiftsbiträdet omedelbart informera den personuppgiftsansvarige om han anser att en instruktion strider mot denna förordning eller mot andra av unionens eller medlemsstaternas dataskyddsbestämmelser.

4. I de fall där ett personuppgiftsbiträde anlitar ett annat personuppgiftsbiträde för utförande av specifik behandling på den personuppgiftsansvariges vägnar ska det andra personuppgiftsbiträdet, genom ett avtal eller en annan rättsakt enligt unionsrätten eller enligt medlemsstaternas nationella rätt, åläggas samma skyldigheter i fråga om dataskydd som de som fastställs i avtalet eller den andra rättsakten mellan den personuppgiftsansvarige och personuppgiftsbiträdet enligt punkt 3, och framför allt att ge tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i denna förordning. Om det andra personuppgiftsbiträdet inte fullgör sina skyldigheter i fråga om dataskydd ska det ursprungliga personuppgiftsbiträdet vara fullt ansvarig gentemot den personuppgiftsansvarige för utförandet av det andra personuppgiftsbiträdets skyldigheter.

5. Ett personuppgiftsbiträdes anslutning till en godkänd uppförandekod som avses i artikel 40 eller en godkänd certifieringsmekanism som avses i artikel 42 får användas för att visa att tillräckliga garantier tillhandahålls, så som avses punkterna 1 och 4 i den här artikeln.

6. Det avtal eller den andra rättsakt som avses i punkterna 3 och 4 i den här artikeln får, utan att det påverkar tillämpningen av ett enskilt avtal mellan den personuppgiftsansvarige och personuppgiftsbiträdet, helt eller delvis baseras på sådana standardavtalsklausuler som avses i punkterna 7 och 8 i den här artikeln, inbegripet när de ingår i en certifiering som i enlighet med artiklarna 42 och 43 beviljats den personuppgiftsansvarige eller personuppgiftsbiträdet.

7. Kommissionen får fastställa standardavtalsklausuler för de frågor som avses i punkterna 3 och 4 i den här artikeln, i enlighet med det granskningsförfarande som avses i artikel 93.2.

8. En tillsynsmyndighet får fastställa standardavtalsklausuler för de frågor som avses i punkterna 3 och 4 i den här artikeln, i enlighet med den mekanism för enhetlighet som avses i artikel 63.

9. Det avtal eller den andra rättsakt som avses i punkterna 3 och 4 ska upprättas skriftligen, inbegripet i ett elektroniskt format.

10. Om ett personuppgiftsbiträde överträder denna förordning genom att fastställa ändamålen med och medlen för behandlingen, ska personuppgiftsbiträdet anses vara personuppgiftsansvarig med avseende på den behandlingen, utan att det påverkar tillämpningen av artiklarna 82, 83 och 84.

Artikel 29

Behandling under den personuppgiftsansvariges eller personuppgiftsbiträdets överinseende

Personuppgiftsbiträdet och personer som utför arbete under den personuppgiftsansvariges eller personuppgiftsbiträdets överinseende, och som får tillgång till personuppgifter, får endast behandla dessa på instruktion från den personuppgiftsansvarige, såvida han eller hon inte är skyldig att göra det enligt unionsrätten eller medlemsstaternas nationella rätt.

Artikel 30

Register över behandling

1. Varje personuppgiftsansvarig och, i tillämpliga fall, dennes företrädare ska föra ett register över behandling som utförts under dess ansvar. Detta register ska innehålla samtliga följande uppgifter:

a) Namn och kontaktuppgifter för den personuppgiftsansvarige, samt i tillämpliga fall gemensamt personuppgiftsansvariga, den personuppgiftsansvariges företrädare samt dataskyddsombudet.

b) Ändamålen med behandlingen.

c) En beskrivning av kategorierna av registrerade och av kategorierna av personuppgifter.

d) De kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut, inbegripet mottagare i tredjeländer eller i internationella organisationer.

e) I tillämpliga fall, överföringar av personuppgifter till ett tredjeland eller en internationell organisation, inbegripet identifiering av tredjelandet eller den internationella organisationen och, vid sådana överföringar som avses i artikel 49.1 andra stycket, dokumentationen av lämpliga skyddsåtgärder.

f) Om möjligt, de förutsedda tidsfristerna för radering av de olika kategorierna av uppgifter.

g) Om möjligt, en allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärder som avses i artikel 32.1.

2. Varje personuppgiftsbiträde och, i tillämpliga fall, dennes företrädare ska föra ett register över alla kategorier av behandling som utförts för den personuppgiftsansvariges räkning, som omfattar följande:

a) Namn och kontaktuppgifter för personuppgiftsbiträdet eller personuppgiftsbiträdena och för varje personuppgiftsansvarig för vars räkning personuppgiftsbiträdet agerar, och, i tillämpliga fall, för den personuppgiftsansvariges eller personuppgiftsbiträdets företrädare samt dataskyddsombudet.

b) De kategorier av behandling som har utförts för varje personuppgiftsansvariges räkning.

c) I tillämpliga fall, överföringar av personuppgifter till ett tredjeland eller en internationell organisation, inbegripet identifiering av tredjelandet eller den internationella organisationen och, vid sådana överföringar som avses i artikel 49.1 andra stycket, dokumentationen av lämpliga skyddsåtgärder.

d) Om möjligt, en allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärder som avses i artikel 32.1.

3. De register som avses i punkterna 1 och 2 ska upprättas skriftligen, inbegripet i elektronisk form.

4. På begäran ska den personuppgiftsansvarige eller personuppgiftsbiträdet samt, i tillämpliga fall, den personuppgiftsansvariges eller personuppgiftsbiträdets företrädare göra registret tillgängligt för tillsynsmyndigheten.

5. De skyldigheter som anges i punkterna 1 och 2 ska inte gälla för ett företag eller en organisation som sysselsätter färre än 250 personer såvida inte den behandling som utförs sannolikt kommer att medföra en risk för registrerades rättigheter och friheter, behandlingen inte är tillfällig eller behandlingen omfattar särskilda kategorier av uppgifter som avses i artikel 9.1 eller personuppgifter om fällande domar i brottmål samt överträdelser som avses i artikel 10.

Artikel 31

Samarbete med tillsynsmyndigheten

Den personuppgiftsansvarige och personuppgiftsbiträdet samt, i tillämpliga fall, deras företrädare ska på begäran samarbeta med tillsynsmyndigheten vid utförandet av dennes uppgifter.

Avsnitt 2

Säkerhet för personuppgifter

Artikel 32

Säkerhet i samband med behandlingen

1. Med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige och personuppgiftsbiträdet vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken, inbegripet, när det är lämpligt

a) pseudonymisering och kryptering av personuppgifter,

b) förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och -tjänsterna,

c) förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident,

d) ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.

2. Vid bedömningen av lämplig säkerhetsnivå ska särskild hänsyn tas till de risker som behandling medför, i synnerhet från oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

3. Anslutning till en godkänd uppförandekod som avses i artikel 40 eller en godkänd certifieringsmekanism som avses i artikel 42 får användas för att visa att kraven i punkt 1 i den här artikeln följs.

4. Den personuppgiftsansvarige och personuppgiftsbiträdet ska vidta åtgärder för att säkerställa att varje fysisk person som utför arbete under den personuppgiftsansvariges eller personuppgiftsbiträdets överinseende, och som får tillgång till personuppgifter, endast behandlar dessa på instruktion från den personuppgiftsansvarige, om inte unionsrätten eller medlemsstaternas nationella rätt ålägger honom eller henne att göra det.

Artikel 33

Anmälan av en personuppgiftsincident till tillsynsmyndigheten

1. Vid en personuppgiftsincident ska den personuppgiftsansvarige utan onödigt dröjsmål och, om så är möjligt, inte senare än 72 timmar efter att ha fått vetskap om den, anmäla personuppgiftsincidenten till den tillsynsmyndighet som är behörig i enlighet med artikel 55, såvida det inte är osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter. Om anmälan till tillsynsmyndigheten inte görs inom 72 timmar ska den åtföljas av en motivering till förseningen.

2. Personuppgiftsbiträdet ska underrätta den personuppgiftsansvarige utan onödigt dröjsmål efter att ha fått vetskap om en personuppgiftsincident.

3. Den anmälan som avses i punkt 1 ska åtminstone

a) beskriva personuppgiftsincidentens art, inbegripet, om så är möjligt, de kategorier av och det ungefärliga antalet registrerade som berörs samt de kategorier av och det ungefärliga antalet personuppgiftsposter som berörs,

b) förmedla namnet på och kontaktuppgifterna för dataskyddsombudet eller andra kontaktpunkter där mer information kan erhållas,

c) beskriva de sannolika konsekvenserna av personuppgiftsincidenten, och

d) beskriva de åtgärder som den personuppgiftsansvarige har vidtagit eller föreslagit för att åtgärda personuppgiftsincidenten, inbegripet, när så är lämpligt, åtgärder för att mildra dess potentiella negativa effekter.

4. Om och i den utsträckning det inte är möjligt att tillhandahålla informationen samtidigt, får informationen tillhandahållas i omgångar utan onödigt ytterligare dröjsmål.

5. Den personuppgiftsansvarige ska dokumentera alla personuppgiftsincidenter, inbegripet omständigheterna kring personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits. Dokumentationen ska göra det möjligt för tillsynsmyndigheten att kontrollera efterlevnaden av denna artikel.

Artikel 34

Information till den registrerade om en personuppgiftsincident

1. Om personuppgiftsincidenten sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige utan onödigt dröjsmål informera den registrerade om personuppgiftsincidenten.

2. Den information till den registrerade som avses i punkt 1 i denna artikel ska innehålla en tydlig och klar beskrivning av personuppgiftsincidentens art och åtminstone de upplysningar och åtgärder som avses i artikel 33.3 b, c och d.

3. Information till den registrerade i enlighet med punkt 1 krävs inte om något av följande villkor är uppfyllt:

a) Den personuppgiftsansvarige har genomfört lämpliga tekniska och organisatoriska skyddsåtgärder och dessa åtgärder tillämpats på de personuppgifter som påverkades av personuppgiftsincidenten, i synnerhet sådana som ska göra uppgifterna oläsbara för alla personer som inte är behöriga att få tillgång till personuppgifterna, såsom kryptering.

b) Den personuppgiftsansvarige har vidtagit ytterligare åtgärder som säkerställer att den höga risk för registrerades rättigheter och friheter som avses i punkt 1 sannolikt inte längre kommer att uppstå.

c) Det skulle inbegripa en oproportionell ansträngning. I så fall ska i stället allmänheten informeras eller en liknande åtgärd vidtas genom vilken de registrerade informeras på ett lika effektivt sätt.

4. Om den personuppgiftsansvarige inte redan har informerat den registrerade om personuppgiftsincidenten får tillsynsmyndigheten, efter att ha bedömt sannolikheten för att personuppgiftsincidenten medför en hög risk, kräva att personuppgiftsbiträdet gör det eller får besluta att något av de villkor som avses i punkt 3 uppfylls.

Avsnitt 3

Konsekvensbedömning avseende dataskydd samt föregående samråd

Artikel 35

Konsekvensbedömning avseende dataskydd

1. Om en typ av behandling, särskilt med användning av ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål, sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige före behandlingen utföra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter. En enda bedömning kan omfatta en serie liknande behandlingar som medför liknande höga risker.

2. Den personuppgiftsansvarige ska rådfråga dataskyddsombudet, om ett sådant utsetts, vid genomförande av en konsekvensbedömning avseende dataskydd.

3. En konsekvensbedömning avseende dataskydd som avses i punkt 1 ska särskilt krävas i följande fall:

a) En systematisk och omfattande bedömning av fysiska personers personliga aspekter som grundar sig på automatisk behandling, inbegripet profilering, och på vilken beslut grundar sig som har rättsliga följder för fysiska personer eller på liknande sätt i betydande grad påverkar fysiska personer.

b) Behandling i stor omfattning av särskilda kategorier av uppgifter, som avses i artikel 9.1, eller av personuppgifter som rör fällande domar i brottmål och överträdelser som avses i artikel 10.

c) Systematisk övervakning av en allmän plats i stor omfattning.

4. Tillsynsmyndigheten ska upprätta och offentliggöra en förteckning över det slags behandlingsverksamheter som omfattas av kravet på en konsekvensbedömning avseende dataskydd i enlighet med punkt 1. Tillsynsmyndigheten ska översända dessa förteckningar till den styrelse som avses i artikel 68.

5. Tillsynsmyndigheten får också upprätta och offentliggöra en förteckning över det slags behandlingsverksamheter som inte kräver någon konsekvensbedömning avseende dataskydd. Tillsynsmyndigheten ska översända dessa förteckningar till styrelsen.

6. Innan de förteckningar som avses i punkterna 4 och 5 antas ska den behöriga tillsynsmyndigheten tillämpa den mekanism för enhetlighet som avses i artikel 63 om en sådan förteckning inbegriper behandling som rör erbjudandet av varor eller tjänster till registrerade, eller övervakning av deras beteende i flera medlemsstater, eller som väsentligt kan påverka den fria rörligheten för personuppgifter i unionen.

7. Bedömningen ska innehålla åtminstone

a) en systematisk beskrivning av den planerade behandlingen och behandlingens syften, inbegripet, när det är lämpligt, den personuppgiftsansvariges berättigade intresse,

b) en bedömning av behovet av och proportionaliteten hos behandlingen i förhållande till syftena,

c) en bedömning av de risker för de registrerades rättigheter och friheter som avses i punkt 1, och

d) de åtgärder som planeras för att hantera riskerna, inbegripet skyddsåtgärder, säkerhetsåtgärder och rutiner för att säkerställa skyddet av personuppgifterna och för att visa att denna förordning efterlevs, med hänsyn till de registrerades och andra berörda personers rättigheter och berättigade intressen.

8. De berörda personuppgiftsansvarigas eller personuppgiftsbiträdenas efterlevnad av godkända uppförandekoder enligt artikel 40 ska på lämpligt sätt beaktas vid bedömningen av konsekvenserna av de behandlingar som utförs av dessa personuppgiftsansvariga eller personuppgiftsbiträden, framför allt när det gäller att ta fram en konsekvensbedömning avseende dataskydd.

9. Den personuppgiftsansvarige ska, när det är lämpligt, inhämta synpunkter från de registrerade eller deras företrädare om den avsedda behandlingen, utan att det påverkar skyddet av kommersiella eller allmänna intressen eller behandlingens säkerhet.

10. Om behandling enligt artikel 6.1 c eller e har en rättslig grund i unionsrätten eller i en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av, reglerar den rätten den aktuella specifika behandlingsåtgärden eller serien av åtgärder i fråga och en konsekvensbedömning avseende dataskydd redan har genomförts som en del av en allmän konsekvensbedömning i samband med antagandet av denna rättsliga grund, ska punkterna 1–7 inte gälla, om inte medlemsstaterna anser det nödvändigt att utföra en sådan bedömning före behandlingen.

11. Den personuppgiftsansvarige ska vid behov genomföra en översyn för att bedöma om behandlingen genomförs i enlighet med konsekvensbedömningen avseende dataskydd åtminstone när den risk som behandlingen medför förändras.

Artikel 36

Förhandssamråd

1. Den personuppgiftsansvarige ska samråda med tillsynsmyndigheten före behandling om en konsekvensbedömning avseende dataskydd enligt artikel 35 visar att behandlingen skulle leda till en hög risk om inte den personuppgiftsansvarige vidtar åtgärder för att minska risken.

2. Om tillsynsmyndigheten anser att den planerade behandling som avses i punkt 1 skulle strida mot denna förordning, särskilt om den personuppgiftsansvarige inte i tillräcklig mån har fastställt eller reducerat risken, ska tillsynsmyndigheten inom en period på högst åtta veckor från det att begäran om samråd mottagits, ge den personuppgiftsansvarige och i tillämpliga fall personuppgiftsbiträdet skriftliga råd och får utnyttja alla de befogenheter som den har enligt artikel 58. Denna period får förlängas med sex veckor beroende på hur komplicerad den planerade behandlingen är. Tillsynsmyndigheten ska informera den personuppgiftsansvarige och, i tillämpliga fall, personuppgiftsbiträdet om en sådan förlängning inom en månad från det att begäran om samråd mottagits, tillsammans med orsakerna till förseningen. Dessa perioder får tillfälligt upphöra att löpa i avvaktan på att tillsynsmyndigheten erhåller den information som den har begärt med tanke på samrådet.

3. Vid samråd med tillsynsmyndigheten enligt punkt 1 ska den personuppgiftsansvarige till tillsynsmyndigheten lämna

a) i tillämpliga fall de respektive ansvarsområdena för de personuppgiftsansvariga, gemensamt personuppgiftsansvariga och personuppgiftsbiträden som medverkar vid behandlingen, framför allt vid behandling inom en koncern,

b) ändamålen med och medlen för den avsedda behandlingen,

c) de åtgärder som vidtas och de garantier som lämnas för att skydda de registrerades rättigheter och friheter enligt denna förordning,

d) i tillämpliga fall kontaktuppgifter till dataskyddsombudet,

e) konsekvensbedömningen avseende dataskydd enligt artikel 35, och

f) all annan information som begärs av tillsynsmyndigheten.

4. Medlemsstaterna ska samråda med tillsynsmyndigheten vid utarbetandet av ett förslag till lagstiftningsåtgärd som ska antas av ett nationellt parlament eller av en regleringsåtgärd som grundar sig på en sådan lagstiftningsåtgärd som rör behandling.

5. Trots vad som sägs i punkt 1 får det i medlemsstaternas nationella rätt krävas att personuppgiftsansvariga ska samråda med, och erhålla förhandstillstånd av, tillsynsmyndigheten när det gäller en personuppgiftsansvarigs behandling för utförandet av en uppgift som den personuppgiftsansvarige utför av allmänt intresse, inbegripet behandling avseende social trygghet och folkhälsa.

Avsnitt 4

Dataskyddsombud

Artikel 37

Utnämning av dataskyddsombudet

1. Den personuppgiftsansvarige och personuppgiftsbiträdet ska under alla omständigheter utnämna ett dataskyddsombud om

a) behandlingen genomförs av en myndighet eller ett offentligt organ, förutom när detta sker som en del av domstolarnas dömande verksamhet,

b) den personuppgiftsansvariges eller personuppgiftsbiträdets kärnverksamhet består av behandling som, på grund av sin karaktär, sin omfattning och/eller sina ändamål, kräver regelbunden och systematisk övervakning av de registrerade i stor omfattning, eller

c) den personuppgiftsansvariges eller personuppgiftsbiträdets kärnverksamhet består av behandling i stor omfattning av särskilda kategorier av uppgifter i enlighet med artikel 9 och personuppgifter som rör fällande domar i brottmål och överträdelser, som avses i artikel 10.

2. En koncern får utnämna ett enda dataskyddsombud om det på varje etableringsort är lätt att nå ett dataskyddsombud.

3. Om den personuppgiftsansvarige eller personuppgiftsbiträdet är en myndighet eller ett offentligt organ, får ett enda dataskyddsombud utnämnas för flera sådana myndigheter eller organ, med hänsyn till deras organisationsstruktur och storlek.

4. I andra fall än de som avses i punkt 1 får eller, om så krävs enligt unionsrätten eller medlemsstaternas nationella rätt, ska den personuppgiftsansvarige eller personuppgiftsbiträdet eller sammanslutningar och andra organ som företräder kategorier av personuppgiftsansvariga eller personuppgiftsbiträden utnämna ett dataskyddsombud. Dataskyddsombudet får agera för sådana sammanslutningar och andra organ som företräder personuppgiftsansvariga eller personuppgiftsbiträden.

5. Dataskyddsombudet ska utses på grundval av yrkesmässiga kvalifikationer och, i synnerhet, sakkunskap om lagstiftning och praxis avseende dataskydd samt förmågan att fullgöra de uppgifter som avses i artikel 39.

6. Dataskyddsombudet får ingå i den personuppgiftsansvariges eller personuppgiftsbiträdets personal, eller utföra uppgifterna på grundval av ett tjänsteavtal.

7. Den personuppgiftsansvarige eller personuppgiftsbiträdet ska offentliggöra dataskyddsombudets kontaktuppgifter och meddela dessa till tillsynsmyndigheten.

Artikel 38

Dataskyddsombudets ställning

1. Den personuppgiftsansvarige och personuppgiftsbiträdet ska säkerställa att dataskyddsombudet på ett korrekt sätt och i god tid deltar i alla frågor som rör skyddet av personuppgifter.

2. Den personuppgiftsansvarige och personuppgiftsbiträdet ska stödja dataskyddsombudet i utförandet av de uppgifter som avses i artikel 39 genom att tillhandahålla de resurser som krävs för att fullgöra dessa uppgifter samt tillgång till personuppgifter och behandlingsförfaranden, samt i upprätthållandet av dennes sakkunskap.

3. Den personuppgiftsansvarige och personuppgiftsbiträdet ska säkerställa att uppgiftskyddsombudet inte tar emot instruktioner som gäller utförandet av dessa uppgifter. Han eller hon får inte avsättas eller bli föremål för sanktioner av den personuppgiftsansvarige eller personuppgiftsbiträdet för att ha utfört sina uppgifter. Dataskyddsombudet ska rapportera direkt till den personuppgiftsansvariges eller personuppgiftsbiträdets högsta förvaltningsnivå.

4. Den registrerade får kontakta dataskyddsombudet med avseende på alla frågor som rör behandlingen av dennes personuppgifter och utövandet av dennes rättigheter enligt denna förordning.

5. Dataskyddsombudet ska, när det gäller dennes genomförande av sina uppgifter, vara bundet av sekretess eller konfidentialitet i enlighet med unionsrätten eller medlemsstaternas nationella rätt.

6. Dataskyddsombudet får fullgöra andra uppgifter och uppdrag. Den personuppgiftsansvarige eller personuppgiftsbiträdet ska se till att sådana uppgifter och uppdrag inte leder till en intressekonflikt.

Artikel 39

Dataskyddsombudets uppgifter

1. Dataskyddsombudet ska ha minst följande uppgifter:

a) Att informera och ge råd till den personuppgiftsansvarige eller personuppgiftsbiträdet och de anställda som behandlar om deras skyldigheter enligt denna förordning och andra av unionens eller medlemsstaternas dataskyddsbestämmelser.

b) Att övervaka efterlevnaden av denna förordning, av andra av unionens eller medlemsstaternas dataskyddsbestämmelser och av den personuppgiftsansvariges eller personuppgiftsbiträdets strategi för skydd av personuppgifter, inbegripet ansvarstilldelning, information till och utbildning av personal som deltar i behandling och tillhörande granskning.

c) Att på begäran ge råd vad gäller konsekvensbedömningen avseende dataskydd och övervaka genomförandet av den enligt artikel 35.

d) Att samarbeta med tillsynsmyndigheten.

e) Att fungera som kontaktpunkt för tillsynsmyndigheten i frågor som rör behandling, inbegripet det förhandssamråd som avses i artikel 36, och vid behov samråda i alla andra frågor.

2. Dataskyddsombudet ska vid utförandet av sina uppgifter ta vederbörlig hänsyn till de risker som är förknippade med behandling, med beaktande av behandlingens art, omfattning, sammanhang och syften.

Avsnitt 5

Uppförandekod och certifiering

Artikel 40

Uppförandekoder

1. Medlemsstaterna, tillsynsmyndigheterna, styrelsen och kommissionen ska uppmuntra utarbetandet av uppförandekoder avsedda att bidra till att denna förordning genomförs korrekt, med hänsyn till särdragen hos de olika sektorer där behandling sker, och de särskilda behoven hos mikroföretag samt små och medelstora företag.

2. Sammanslutningar och andra organ som företräder kategorier av personuppgiftsansvariga eller personuppgiftsbiträden får utarbeta uppförandekoder, eller ändra eller utöka sådana koder, i syfte att specificera tillämpningen av denna förordning, till exempel när det gäller

a) rättvis och öppen behandling,

b) personuppgiftsansvarigas berättigade intressen i särskilda sammanhang,

c) insamling av personuppgifter,

d) pseudonymisering av personuppgifter,

e) information till allmänheten och de registrerade,

f) utövande av registrerades rättigheter,

g) information till och skydd av barn samt metoderna för att erhålla samtycke från de personer som har föräldraansvar för barn,

h) åtgärder och förfaranden som avses i artiklarna 24 och 25 samt åtgärder för att säkerställa säkerhet vid behandling i enlighet med artikel 32,

i) anmälan av personuppgiftsincidenter till tillsynsmyndigheter och meddelande av sådana personuppgiftsincidenter till registrerade,

j) överföring av personuppgifter till tredjeländer eller internationella organisationer,

k) utomrättsliga förfaranden och andra tvistlösningsförfaranden för lösande av tvister mellan personuppgiftsansvariga och registrerade när det gäller behandling, utan att detta påverkar registrerades rättigheter enligt artiklarna 77 och 79.

3. Uppförandekoder som är godkända i enlighet med punkt 5 i denna artikel och som har allmän giltighet enligt punkt 9 i denna artikel får, förutom att de iakttas av personuppgiftsansvariga eller personuppgiftsbiträden som omfattas av denna förordning, även iakttas av personuppgiftsansvariga eller personuppgiftsbiträden som inte omfattas av denna förordning enligt artikel 3, för att tillhandahålla lämpliga garantier inom ramen för överföringar av personuppgifter till tredjeländer eller internationella organisationer enligt villkoren i artikel 46.2 e. Sådana personuppgiftsansvariga eller personuppgiftsbiträden ska göra bindande och verkställbara åtaganden, genom avtal eller andra rättsligt bindande instrument, att tillämpa dessa lämpliga garantier inbegripet när det gäller registrerades rättigheter.

4. Den uppförandekod som avses i punkt 2 i den här artikeln ska innehålla mekanismer som gör det möjligt för det organ som avses i artikel 41.1 att utföra den obligatoriska övervakningen av att dess bestämmelser efterlevs av personuppgiftsansvariga och personuppgiftsbiträden som tillämpar den, utan att det påverkar uppgifter eller befogenheter för de tillsynsmyndigheter som är behöriga enligt artikel 55 eller 56.

5. Sammanslutningar och andra organ som avses i punkt 2 i den här artikeln som avser att utarbeta en uppförandekod eller ändra eller utöka befintliga uppförandekoder ska inge utkastet till uppförandekod, ändringen eller utökningen till den tillsynsmyndighet som är behörig enligt artikel 55. Tillsynsmyndigheten ska yttra sig om huruvida utkastet till uppförandekod, ändring eller utökning överensstämmer med denna förordning och ska godkänna ett det utkastet till kod, ändring eller utökning om den finner att tillräckliga garantier tillhandahålls.

6. Om utkastet till kod, eller en ändring eller utökning, godkänns i enlighet med punkt 5, och om den berörda uppförandekoden inte avser behandling i flera medlemsstater, ska tillsynsmyndigheten registrera och offentliggöra uppförandekoden.

7. Om ett utkast till uppförandekod avser behandling i flera medlemsstater ska den tillsynsmyndighet som är behörig enligt artikel 55 innan den godkänner utkastet till kod, ändring eller utökning, inom ramen för det förfarande som avses i artikel 63 överlämna det till styrelsen som ska avge ett yttrande om huruvida utkastet till kod, ändring eller utökning är förenlig med denna förordning eller, i de fall som avses i punkt 3 i den här artikeln, tillhandahåller lämpliga garantier.

8. Om det i det yttrande som avses i punkt 7 bekräftas att utkastet till kod, ändring eller utökning är förenligt med denna förordning, eller, i de fall som avses i punkt 3, tillhandahåller lämpliga garantier, ska styrelsen inlämna sitt yttrande till kommissionen.

9. Kommissionen får, genom genomförandeakter, besluta att den godkända koden, ändringen eller utökningen som getts in till den enligt punkt 8 i den här artikeln har allmän giltighet inom unionen. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 93.2.

10. Kommissionen ska se till att de godkända koder om vilka det har beslutats att de har allmän giltighet enligt punkt 9 offentliggörs på lämpligt sätt.

11. Styrelsen ska samla alla godkända uppförandekoder, ändringar och utökningar i ett register och offentliggöra dem på lämpligt sätt.

Artikel 41

Övervakning av godkända uppförandekoder

1. Utan att det påverkar den berörda tillsynsmyndighetens uppgifter och befogenheter enligt artiklarna 57 och 58 får övervakningen av efterlevnaden av en uppförandekod i enlighet med artikel 40 utföras av ett organ som har en lämplig expertnivå i förhållande till kodens syfte och som ackrediteras för detta ändamål av den behöriga tillsynsmyndigheten.

2. Ett organ som avses i punkt 1 får ackrediteras för att övervaka efterlevnaden av en uppförandekod om detta organ har

a) visat sitt oberoende och sin expertis i förhållande till uppförandekodens syfte på ett sätt som den behöriga tillsynsmyndigheten finner tillfredsställande,

b) upprättat förfaranden varigenom det kan bedöma de berörda personuppgiftsansvarigas och personuppgiftsbiträdenas lämplighet för att tillämpa uppförandekoden, övervaka att de efterlever dess bestämmelser och regelbundet se över hur den fungerar,

c) upprättat förfaranden och strukturer för att hantera klagomål om överträdelser av uppförandekoden eller det sätt på vilket uppförandekoden har tillämpats, eller tillämpas, av en personuppgiftsansvarig eller ett personuppgiftsbiträde, och för att göra dessa förfaranden och strukturer synliga för registrerade och för allmänheten, och

d) på ett sätt som den behöriga tillsynsmyndigheten finner tillfredsställande visat att dess uppgifter och uppdrag inte leder till en intressekonflikt.

3. Den behöriga tillsynsmyndigheten ska inlämna utkastet till kriterier för ackreditering av ett organ som avses i punkt 1 i den här artikeln till styrelsen i enlighet med den mekanism för enhetlighet som avses i artikel 63.

4. Utan att det påverkar den behöriga tillsynsmyndighetens uppgifter och befogenheter och tillämpningen av bestämmelserna i kapitel VIII ska ett organ som avses i punkt 1 i denna artikel, med förbehåll för tillräckliga skyddsåtgärder, vidta lämpliga åtgärder i fall av en personuppgiftsansvarigs eller ett personuppgiftsbiträdes överträdelse av uppförandekoden, inbegripet avstängning eller uteslutande av den personuppgiftsansvarige eller personuppgiftsbiträdet från uppförandekoden. Det ska informera den behöriga tillsynsmyndigheten om sådana åtgärder och skälen för att de vidtagits.

5. Den behöriga tillsynsmyndigheten ska återkalla ackrediteringen av ett organ som avses i punkt 1 om villkoren för ackrediteringen inte, eller inte längre, uppfylls eller om åtgärder som vidtagits av organet strider mot denna förordning.

6. Denna artikel ska inte gälla behandling som utförs av offentliga myndigheter och organ.

Artikel 42

Certifiering

1. Medlemsstaterna, tillsynsmyndigheterna, styrelsen och kommissionen ska uppmuntra, särskilt på unionsnivå, införandet av certifieringsmekanismer för dataskydd och sigill och märkningar för dataskydd som syftar till att visa att personuppgiftsansvarigas eller personuppgiftsbiträdens behandling är förenlig med denna förordning. De särskilda behoven hos mikroföretag samt små och medelstora företag ska beaktas.

2. Certifieringsmekanismer för dataskydd och sigill och märkningar för dataskydd som är godkända enligt punkt 5 i denna artikel får, förutom att de iakttas av personuppgiftsansvariga eller personuppgiftsbiträden som omfattas av denna förordning, inrättas för att visa att det föreligger lämpliga garantier som tillhandahålls av personuppgiftsansvariga och personuppgiftsbiträden som inte omfattas av denna förordning enligt artikel 3, inom ramen för överföringar av personuppgifter till tredjeländer eller internationella organisationer enligt villkoren i artikel 46.2 f. Sådana personuppgiftsansvariga eller personuppgiftsbiträden ska göra bindande och verkställbara åtaganden, genom avtal eller andra rättsligt bindande instrument, att tillämpa dessa lämpliga garantier, inbegripet när det gäller registrerades rättigheter.

3. Certifieringen ska vara frivillig och tillgänglig via ett öppet förfarande.

4. En certifiering i enlighet med denna artikel minskar inte den personuppgiftsansvariges eller personuppgiftsbiträdets ansvar för att denna förordning efterlevs och påverkar inte uppgifter och befogenheter för de tillsynsmyndigheter som är behöriga enligt artikel 55 eller 56.

5. En certifiering i enlighet med denna artikel ska utfärdas av de certifieringsorgan som avses i artikel 43 eller av den behöriga tillsynsmyndigheten på grundval av kriterier som godkänts av den behöriga myndigheten enligt artikel 58.3 eller av styrelsen enligt artikel 63. Om kriterierna har godkänts av styrelsen får detta leda till en gemensam certifiering, det europeiska sigillet för dataskydd.

6. Den personuppgiftsansvarige eller det personuppgiftsbiträde som låter sin behandling av uppgifter omfattas av certifieringsmekanismen ska förse det certifieringsorgan som avses i artikel 43 eller, i tillämpliga fall, den behöriga tillsynsmyndigheten, med all information och tillgång till behandlingsförfaranden som krävs för att genomföra certifieringsförfarandet.

7. Certifiering ska utfärdas till en personuppgiftsansvarig eller ett personuppgiftsbiträde för en period på högst tre år och får förnyas på samma villkor under förutsättning att kraven fortsätter att vara uppfyllda. Certifiering ska, i tillämpliga fall, återkallas av de certifieringsorgan som avses i artikel 43 eller av den behöriga tillsynsmyndigheten om kraven för certifieringen inte eller inte längre uppfylls.

8. Styrelsen ska samla alla certifieringsmekanismer och sigill och märkningar för dataskydd i ett register och offentliggöra dem på lämpligt sätt.

Artikel 43

Certifieringsorgan

1. Utan att det påverkar den behöriga tillsynsmyndighetens uppgifter och befogenheter enligt artiklarna 57 och 58 ska certifieringsorgan som har lämplig nivå av expertis i fråga om dataskydd, efter att ha informerat tillsynsmyndigheten för att den ska kunna utöva sina befogenheter enligt artikel 58.2 h när så är nödvändigt, utfärda och förnya certifiering. Medlemsstat ska säkerställa att dessa certifieringsorgan är ackrediterade av en av eller båda följande:

a) Den tillsynsmyndighet som är behörig enligt artikel 55 eller 56,

b) det nationella ackrediteringsorgan som utsetts i enlighet med Europaparlamentets och rådets förordning (EG) nr 765/2008 ([1]) i enlighet med EN-ISO/IEC 17065/2012 och med de ytterligare krav som fastställts av den tillsynsmyndighet som är behörig enligt artikel 55 eller 56.

2. Certifieringsorgan som avses i punkt 1 får ackrediteras i enlighet med den punkten endast om de har

a) visat oberoende och expertis i förhållande till certifieringens syfte på ett sätt som den behöriga tillsynsmyndigheten finner tillfredsställande,

([1]) Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93 (EUT L 218, 13.8.2008, s. 30).

b) förbundit sig att respektera de kriterier som avses i artikel 42.5 och godkänts av den tillsynsmyndighet som är behörig enligt artikel 55 eller 56, eller av styrelsen enligt artikel 63,

c) upprättat förfaranden för utfärdande, periodisk översyn och återkallande av certifiering, sigill och märkningar för dataskydd,

d) upprättat förfaranden och strukturer för att hantera klagomål om överträdelser av certifieringen eller det sätt på vilket certifieringen har tillämpats, eller tillämpas, av en personuppgiftsansvarig eller ett personuppgiftsbiträde, och för att göra dessa förfaranden och strukturer synliga för registrerade och för allmänheten, och

e) på ett sätt som den behöriga tillsynsmyndigheten finner tillfredsställande visat att deras uppgifter och uppdrag inte leder till en intressekonflikt.

3. Ackrediteringen av certifieringsorgan som avses i punkterna 1 och 2 i denna artikel ska ske på grundval av kriterier som godkänts av den tillsynsmyndighet som är behörig enligt artikel 55 eller 56, eller av styrelsen enligt artikel 63. I händelse av ackreditering enligt punkt 1 b i den här artikeln ska dessa krav komplettera dem som föreskrivs i förordning (EG) nr 765/2008 och de tekniska regler som beskriver certifieringsorganens metoder och förfaranden.

4. De certifieringsorgan som avses i punkt 1 ska ansvara för den korrekta bedömning som leder till certifieringen eller återkallelsen av certifieringen, utan att det påverkar den personuppgiftsansvariges eller personuppgiftsbiträdets ansvar att efterleva denna förordning. Ackrediteringen ska utfärdas för en period på högst fem år och får förnyas på samma villkor under förutsättning att certifieringsorganet uppfyller de krav som anges i denna artikel.

5. De certifieringsorgan som avses i punkt 1 ska informera de behöriga tillsynsmyndigheterna om orsakerna till beviljandet eller återkallelsen av den begärda certifieringen.

6. De krav som avses i punkt 3 i den här artikeln och de kriterier som avses i artikel 42.5 ska offentliggöras av tillsynsmyndigheten i ett lättillgängligt format. Tillsynsmyndigheterna ska också översända dessa krav och kriterier till styrelsen. Styrelsen ska samla alla certifieringsmekanismer och sigill för dataskydd i ett register och offentliggöra dem på lämpligt sätt.

7. Utan att det påverkar tillämpningen av kapitel VIII ska den behöriga tillsynsmyndigheten eller det nationella ackrediteringsorganet återkalla ett certifieringsorgans ackreditering enligt punkt 1 i denna artikel om villkoren för ackrediteringen inte, eller inte längre, uppfylls eller om åtgärder som vidtagits av certifieringsorganet strider mot denna förordning.

8. Kommissionen ska ges befogenhet att anta delegerade akter i enlighet med artikel 92 i syfte att närmare ange de krav som ska tas i beaktande för de certifieringsmekanismer för dataskydd som avses i artikel 42.1.

9. Kommissionen får anta genomförandeakter för att fastställa tekniska standarder för certifieringsmekanismer och sigill och märkningar för dataskydd samt rutiner för att främja och erkänna dessa certifieringsmekanismer, sigill och märkningar. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 93.2.

KAPITEL V

Överföring av personuppgifter till tredjeländer eller internationella organisationer

Artikel 44

Allmän princip för överföring av uppgifter

Överföring av personuppgifter som är under behandling eller är avsedda att behandlas efter det att de överförts till ett tredjeland eller en internationell organisation får bara ske under förutsättning att den personuppgiftsansvarige och personuppgiftsbiträdet, med förbehåll för övriga bestämmelser i denna förordning, uppfyller villkoren i detta kapitel, inklusive för vidare överföring av personuppgifter från tredjelandet eller den internationella organisationen till ett annat tredjeland eller en annan internationell organisation. Alla bestämmelser i detta kapitel ska tillämpas för att säkerställa att den nivå på skyddet av fysiska personer som säkerställs genom denna förordning inte undergrävs.

Artikel 45

Överföring på grundval av ett beslut om adekvat skyddsnivå

1. Personuppgifter får överföras till ett tredjeland eller en internationell organisation om kommissionen har beslutat att tredjelandet, ett territorium eller en eller flera specificerade sektorer i tredjelandet, eller den internationella organisationen i fråga säkerställer en adekvat skyddsnivå. En sådan överföring ska inte kräva något särskilt tillstånd.

2. När kommissionen bedömer om en adekvat skyddsnivå föreligger ska den särskilt beakta

a) rättsstatsprincipen, respekten för de mänskliga rättigheterna och de grundläggande friheterna, relevant lagstiftning, både allmän lagstiftning och sektorslagstiftning, inklusive avseende allmän säkerhet, försvar, nationell säkerhet och straffrätt och offentliga myndigheters tillgång till personuppgifter samt tillämpningen av sådan lagstiftning, dataskyddsregler, yrkesregler och säkerhetsbestämmelser, inbegripet regler för vidare överföring av personuppgifter till ett annat tredjeland eller en annan internationell organisation, som ska följas i det landet eller den internationella organisationen, rättspraxis samt faktiska och verkställbara rättigheter för registrerade och effektiv administrativ och rättslig prövning för de registrerade vars personuppgifter överförs,

b) huruvida det finns en eller flera effektivt fungerande oberoende tillsynsmyndigheter i tredjelandet, eller som utövar tillsyn över den internationella organisationen, som har ansvar för att säkerställa och kontrollera att dataskyddsregler följs, inklusive lämpliga verkställighetsbefogenheter, ge de registrerade råd och assistans när det gäller utövandet av deras rättigheter och samarbeta med medlemsstaternas tillsynsmyndigheter, och

c) vilka internationella åtaganden det berörda tredjelandet eller den berörda internationella organisationen har gjort, eller andra skyldigheter som följer av rättsligt bindande konventioner eller instrument samt av dess deltagande i multilaterala eller regionala system, särskilt rörande skydd av personuppgifter.

3. Kommissionen får, efter att ha bedömt om det föreligger en adekvat skyddsnivå, genom en genomförandeakt besluta att ett tredjeland, ett territorium eller en eller flera specificerade sektorer inom ett tredjeland, eller en internationell organisation säkerställer en adekvat skyddsnivå i den mening som avses i punkt 2 i den här artikeln. Genomförandeakten ska inrätta en mekanism för regelbunden översyn, minst vart fjärde år, som ska beakta all relevant utveckling i det tredjelandet eller den internationella organisationen. Beslutets territoriella och sektorsmässiga tillämpning ska regleras i genomförandeakten, där det också i förekommande fall ska anges vilken eller vilka myndigheter som är tillsynsmyndighet(er) enligt punkt 2 b i den här artikeln. Genomförandeakten ska antas i enlighet med det granskningsförfarande som avses i artikel 93.2.

4. Kommissionen ska fortlöpande övervaka utveckling i tredjeländer och internationella organisationer vilken kan påverka hur beslut som antagits enligt punkt 3 i den här artikeln och beslut som antagits på grundval av artikel 25.6 i direktiv 95/46/EG fungerar.

5. Kommissionen ska, när tillgänglig information visar, i synnerhet efter den översyn som avses i punkt 3 i den här artikeln, att ett tredjeland, ett territorium eller en eller flera specificerade sektorer inom tredjelandet i fråga eller en internationell organisation inte längre säkerställer adekvat skydd i den mening som avses i punkt 2 i den här artikeln och, i den mån det behövs, genom genomförandeakter återkalla, ändra eller upphäva det beslut som avses i punkt 3 i den här artikeln utan retroaktiv verkan. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 93.2.

När det föreligger vederbörligen motiverade och tvingande skäl till skyndsamhet ska kommissionen anta omedelbart tillämpliga genomförandeakter i enlighet med det förfarande som avses i artikel 93.3.

6. Kommissionen ska samråda med tredjelandet eller den internationella organisationen i fråga för att lösa den situation som lett till beslutet enligt punkt 5.

7. Beslut enligt punkt 5 i den här artikeln ska inte påverka överföring av personuppgifter till tredjelandet, ett territorium eller en eller flera specificerade sektorer inom tredjelandet, eller den internationella organisationen i fråga enligt artiklarna 46–49.

8. Kommissionen ska i *Europeiska unionens officiella tidning* och på sin webbplats offentliggöra en förteckning över de tredjeländer och de territorier och specificerade sektorer i ett givet tredjeland samt de internationella organisationer för vilka den har fastställt att en adekvat skyddsnivå inte eller inte längre säkerställs.

9. De beslut som antas av kommissionen på grundval av artikel 25.6 i direktiv 95/46/EG ska förbli i kraft tills de ändrats, ersatts eller upphävts av ett kommissionsbeslut som antagits i enlighet med punkt 3 eller 5 i den här artikeln.

Artikel 46

Överföring som omfattas av lämpliga skyddsåtgärder

1. I avsaknad av ett beslut i enlighet med artikel 45.3, får en personuppgiftsansvarig eller ett personuppgiftsbiträde endast överföra personuppgifter till ett tredjeland eller en internationell organisation efter att ha vidtagit lämpliga skyddsåtgärder, och på villkor att lagstadgade rättigheter för registrerade och effektiva rättsmedel för registrerade finns tillgängliga.

2. Lämpliga skyddsåtgärder enligt punkt 1 får, utan att det krävs särskilt tillstånd från en övervakningsmyndighet, ta formen av

a) ett rättsligt bindande och verkställbart instrument mellan offentliga myndigheter eller organ,

b) bindande företagsbestämmelser i enlighet med artikel 47,

c) standardiserade dataskyddsbestämmelser som antas av kommissionen i enlighet med det granskningsförfarande som avses i artikel 93.2,

d) standardiserade dataskyddsbestämmelser som antagits av en tillsynsmyndighet och godkänts av kommissionen i enlighet med det granskningsförfarande som avses i artikel 93.2,

e) en godkänd uppförandekod enlig artikel 40 tillsammans med rättsligt bindande och verkställbara åtaganden för den personuppgiftsansvarige eller personuppgiftsbiträdet i tredjelandet att tillämpa lämpliga skyddsåtgärder, även när det gäller registrerades rättigheter, eller

f) en godkänd certifieringsmekanism enlig artikel 42 tillsammans med rättsligt bindande och verkställbara åtaganden för den personuppgiftsansvarige, personuppgiftsbiträdet i tredjelandet att tillämpa lämpliga skyddsåtgärder, även när det gäller de registrerades rättigheter.

3. Med förbehåll för tillstånd från den behöriga tillsynsmyndigheten, får lämpliga skyddsåtgärder enligt punkt 1 också i synnerhet ta formen av

a) avtalsklausuler mellan den personuppgiftsansvarige eller personuppgiftsbiträdet och den personuppgiftsansvarige, personuppgiftsbiträdet eller mottagaren av personuppgifterna i tredjelandet eller den internationella organisationen, eller

b) bestämmelser som ska införas i administrativa överenskommelser mellan offentliga myndigheter eller organ vilka inbegriper verkställbara och faktiska rättigheter för registrerade.

4. Tillsynsmyndigheten ska tillämpa den mekanism för enhetlighet som avses i artikel 63 i de fall som avses i punkt 3 i den här artikeln.

5. Tillstånd från en medlemsstat eller tillsynsmyndighet på grundval av artikel 26.2 i direktiv 95/46/EG ska förbli giltigt tills det, vid behov, ändrats, ersatts eller upphävts av den tillsynsmyndigheten. De beslut som fattas av kommissionen på grundval av artikel 26.4 i direktiv 95/46/EG ska förbli i kraft tills de, vid behov, ändrats, ersatts eller upphävts av ett kommissionsbeslut som antagits i enlighet med punkt 2 i den här artikeln.

Artikel 47

Bindande företagsbestämmelser

1. Den behöriga tillsynsmyndigheten ska godkänna bindande företagsbestämmelser i enlighet med den mekanism för enhetlighet som föreskrivs i artikel 63 under förutsättning att de

a) är rättslig bindande, tillämpas på, och verkställs av alla delar som berörs inom den koncern eller grupp av företag som deltar i gemensam ekonomisk verksamhet, inklusive deras anställda,

b) innehåller uttryckliga bestämmelser om de registrerades lagstadgade rättigheter när det gäller behandlingen av deras personuppgifter, och

c) uppfyller villkoren i punkt 2.

2. De bindande företagsbestämmelser som avses i punkt 1 ska närmare ange åtminstone följande:

a) struktur och kontaktuppgifter för den koncern eller grupp av företag som deltar i gemensam ekonomisk verksamhet och för var och en av dess medlemmar,

b) vilka överföringar eller uppsättningar av överföringar av uppgifter som omfattas, inklusive kategorierna av personuppgifter, typen av behandling och dess ändamål, den typ av registrerade som berörs samt vilket eller vilka tredjeländer som avses,

c) bestämmelsernas rättsligt bindande natur, såväl internt som externt,

d) tillämpningen av allmänna principer för dataskydd, särskilt avgränsning av syften, uppgiftsminimering, begränsade lagringsperioder, datakvalitet, inbyggt dataskydd och dataskydd som standard, rättslig grund för behandling, behandling av särskilda kategorier av personuppgifter, åtgärder för att säkerställa datasäkerhet och villkoren när det gäller vidare överföring av uppgifter till organ som inte är bundna av bindande företagsbestämmelser,

e) de registrerades rättigheter avseende behandling och medlen för att utöva dessa rättigheter, inklusive rätten att inte bli föremål för beslut grundade enbart på automatisk behandling, inklusive profilering, enligt artikel 22, rätten att inge klagomål till den behöriga tillsynsmyndigheten och till behöriga domstolar i medlemsstaterna enligt artikel 79, rätten till prövning samt i förekommande fall rätten till kompensation för överträdelse av de bindande företagsbestämmelserna,

f) att den personuppgiftsansvarige eller personuppgiftsbiträdet som är etablerad inom en medlemsstats territorium tar på sig ansvaret om en berörd enhet som inte är etablerad inom unionen bryter mot de bindande företagsbestämmelserna; den personuppgiftsansvarige eller personuppgiftsbiträdet får helt eller delvis undantas från denna skyldighet endast på villkor att det kan visas att den berörda enheten i företagsgruppen inte kan hållas ansvarig för den skada som har uppkommit,

g) hur de registrerade ska informeras om innehållet i de bindande företagsbestämmelserna, särskilt de bestämmelser som avses i leden d, e och f i denna punkt utöver den information som avses i artiklarna 13 och 14,

h) uppgifterna för varje dataskyddsombud som utsetts i enlighet med artikel 37, eller varje annan person eller enhet med ansvar för kontrollen av att de bindande företagsbestämmelserna följs inom den koncern eller grupp av företag som deltar i gemensam ekonomisk verksamhet, samt i fråga om utbildning och hantering av klagomål,

i) förfaranden för klagomål,

j) rutinerna inom den koncern eller grupp av företag som deltar i gemensam ekonomisk verksamhet för att kontrollera att de bindande företagsreglerna följs; sådana rutiner ska inbegripa dataskyddstillsyn och metoder för att säkerställa korrigerande åtgärder för att skydda de registrerades rättigheter; resultaten av sådana kontroller bör meddelas den person eller enhet som avses i led h och styrelsen i det kontrollerande företaget i koncernen eller gruppen av företag som deltar i gemensam ekonomisk verksamhet, och bör på begäran vara tillgänglig för den behöriga tillsynsmyndigheten,

k) rutinerna för att rapportera och dokumentera ändringar i bestämmelserna, samt rutinerna för att rapportera dessa ändringar till tillsynsmyndigheten,

l) rutinerna för att samarbeta med tillsynsmyndigheten i syfte att se till att alla medlemmar i den koncern eller grupp av företag som deltar i gemensam ekonomisk verksamhet följer reglerna, särskilt genom att meddela tillsynsmyndigheten resultaten av kontroller av de åtgärder som avses i led j,

m) rutinerna för att till den behöriga tillsynsmyndigheten rapportera alla rättsliga krav som en medlem i koncernen eller gruppen av företag som deltar i gemensam ekonomisk verksamhet är underkastad i ett tredjeland och som sannolikt kommer att ha en avsevärd negativ inverkan på de garantier som ges genom de bindande företagsbestämmelserna, och

n) lämplig utbildning om dataskydd för personal som har ständig eller regelbunden tillgång till personuppgifter.

3. Kommissionen får närmare ange vilket format och vilka rutiner som ska användas för de personuppgiftsansvarigas, personuppgiftsbiträdenas och tillsynsmyndigheternas utbyte av information om bindande företagsbestämmelser i den mening som avses i denna artikel. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 93.2.

Artikel 48

Överföringar och utlämnanden som inte är tillåtna enligt unionsrätten

Domstolsbeslut eller beslut från myndigheter i tredjeland där det krävs att en personuppgiftsansvarig eller ett personuppgiftsbiträde överför eller lämnar ut personuppgifter får erkännas eller genomföras på något som helst sätt endast om det grundar sig på en internationell överenskommelse, såsom ett avtal om ömsesidig rättslig hjälp, som gäller mellan det begärande tredjelandet och unionen eller en medlemsstat, utan att detta påverkar andra grunder för överföring enligt detta kapitel.

Artikel 49

Undantag i särskilda situationer

1. Om det inte föreligger något beslut om adekvat skyddsnivå enligt artikel 45.3, eller om lämpliga skyddsåtgärder enligt artikel 46, inbegripet bindande företagsbestämmelser, får en överföring eller uppsättning av överföringar av personuppgifter till ett tredjeland eller en internationell organisation endast ske om något av följande villkor är uppfyllt:

a) Den registrerade har uttryckligen samtyckt till att uppgifterna får överföras, efter att först ha blivit informerad om de eventuella riskerna med sådana överföringar för den registrerade när det inte föreligger något beslut om adekvat skyddsnivå eller lämpliga skyddsåtgärder.

b) Överföringen är nödvändig för att fullgöra ett avtal mellan den registrerade och den personuppgiftsansvarige eller för att genomföra åtgärder som föregår ett sådant avtal på den registrerades begäran.

c) Överföringen är nödvändig för att ingå eller fullgöra ett avtal mellan den personuppgiftsansvarige och en annan fysisk eller juridisk person i den registrerades intresse.

d) Överföringen är nödvändig av viktiga skäl som rör allmänintresset.

e) Överföringen är nödvändig för att kunna fastställa, göra gällande eller försvara rättsliga anspråk.

f) Överföringen är nödvändig för att skydda den registrerades eller andra personers grundläggande intressen, när den registrerade är fysiskt eller rättsligt förhindrad att ge sitt samtycke.

g) Överföringen görs från ett register som enligt unionsrätten eller medlemsstaternas nationella rätt är avsett att ge allmänheten information och som är tillgängligt antingen för allmänheten eller för var och en som kan styrka ett berättigat intresse, men endast i den utsträckning som de i unionsrätten eller i medlemsstaternas nationella rätt angivna villkoren för tillgänglighet uppfylls i det enskilda fallet.

När en överföring inte skulle kunna grundas på en bestämmelse i artikel 45 eller 46, inklusive bestämmelserna om bindande företagsbestämmelser, och inget av undantagen för en särskild situation som avses i första stycket i den här punkten är tillämpligt, får en överföring till ett tredjeland eller en internationell organisation äga rum endast omöverföringen inte är repetitiv, endast gäller ett begränsat antal registrerade, är nödvändig för ändamål som rör den personuppgiftsansvariges tvingande berättigade intressen och den registrerades intressen eller rättigheter och friheter inte väger tyngre, och den personuppgiftsansvarige har bedömt samtliga omständigheter kring överföringen av uppgifter och på grundval av denna bedömning vidtagit lämpliga skyddsåtgärder för att skydda personuppgifter. Den personuppgiftsansvarige ska informera tillsynsmyndigheten om överföringen. Den personuppgiftsansvarige ska utöver tillhandahållande av den information som avses i artiklarna 13 och 14 informera den registrerade om överföringen och om de tvingande berättigade intressen som eftersträvas.

2. En överföring enligt led g i punkt 1 första stycket får inte 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.

3. Leden a, b och c i punkt 1 första stycket samt andra stycket i samma punkt ska inte gälla åtgärder som vidtas av offentliga myndigheter som ett led i myndighetsutövning.

4. Det allmänintresse som avses i led d i punkt 1 första stycket ska vara erkänt i unionsrätten eller i den nationella rätt som den personuppgiftsansvarige omfattas av.

5. Saknas beslut om adekvat skyddsnivå, får unionsrätten eller medlemsstaternas nationella rätt med hänsyn till viktiga allmänintressen uttryckligen fastställa gränser för överföringen av specifika kategorier av personuppgifter till ett tredjeland eller en internationell organisation. Medlemsstaterna ska underrätta kommissionen om sådana bestämmelser.

6. Den personuppgiftsansvarige eller personuppgiftsbiträdet ska bevara uppgifter både om bedömningen och om de lämpliga skyddsåtgärder som avses i punkt 1 andra stycket i den här artikeln i det register som avses i artikel 30.

Artikel 50

Internationellt samarbete för skydd av personuppgifter

När det gäller tredjeländer och internationella organisationer ska kommissionen och tillsynsmyndigheterna vidta lämpliga åtgärder för att

a) utveckla rutiner för det internationella samarbetet för att underlätta en effektiv tillämpning av lagstiftningen om skydd av personuppgifter,

b) på internationell nivå erbjuda ömsesidigt bistånd för en effektiv tillämpning av lagstiftningen om skydd av personuppgifter, bland annat genom underrättelse, hänskjutande av klagomål, bistånd vid utredningar samt informationsutbyte, med iakttagande av lämpliga skyddsåtgärder för personuppgifter samt skyddet av andra grundläggande rättigheter och friheter,

c) involvera berörda aktörer i diskussioner och åtgärder som syftar till att öka det internationella samarbetet när det gäller tillämpningen av lagstiftningen om skydd av personuppgifter,

d) främja utbyte och dokumentation om lagstiftning och praxis för skydd av personuppgifter, inklusive avseende behörighetskonflikter med tredjeländer.

KAPITEL VI

Oberoende tillsynsmyndigheter

Avsnitt 1

Oberoende ställning

Artikel 51

Tillsynsmyndighet

1. Varje medlemsstat ska föreskriva att en eller flera offentliga myndigheter ska vara ansvariga för att övervaka tillämpningen av denna förordning, i syfte att skydda fysiska personers grundläggande rättigheter och friheter i samband med behandling samt att underlätta det fria flödet av sådana uppgifter inom unionen (nedan kallad *tillsynsmyndighet*).

2. Varje tillsynsmyndighet ska bidra till en enhetlig tillämpning av denna förordning i hela unionen. För detta ändamål ska tillsynsmyndigheterna samarbeta såväl sinsemellan som med kommissionen i enlighet med kapitel VII.

3. Om det finns fler än en tillsynsmyndighet i en medlemsstat ska medlemsstaten utse den tillsynsmyndighet som ska företräda dessa myndigheter i styrelsen; medlemsstaten ska också upprätta en rutin för att se till att övriga myndigheter följer reglerna för den mekanism för enhetlighet som avses i artikel 63.

4. Varje medlemsstat ska senast den 25 maj 2018 anmäla till kommissionen vilka nationella bestämmelser den antar i enlighet med detta kapitel, och alla framtida ändringar som rör dessa bestämmelser ska anmälas utan dröjsmål.

Artikel 52

Oberoende

1. Varje tillsynsmyndighet ska vara fullständigt oberoende i utförandet av sina uppgifter och utövandet av sina befogenheter i enlighet med denna förordning.

2. Varje tillsynsmyndighets ledamot eller ledamöter ska i utförandet av sina uppgifter och utövandet av sina befogenheter i enlighet med denna förordning stå fria från utomstående påverkan, direkt såväl som indirekt, och får varken begära eller ta emot instruktioner av någon.

3. Tillsynsmyndighetens ledamöter ska avhålla sig från alla handlingar som är oförenliga med deras skyldigheter och under sin mandattid avstå från all annan avlönad eller oavlönad yrkesverksamhet som står i strid med deras tjänsteutövning.

4. Varje medlemsstat ska säkerställa att varje tillsynsmyndighet förfogar över de personella, tekniska och finansiella resurser samt de lokaler och den infrastruktur som behövs för att myndigheten ska kunna utföra sina uppgifter och utöva sina befogenheter, inklusive inom ramen för det ömsesidiga biståndet, samarbetet och deltagandet i styrelsens verksamhet.

5. Varje medlemsstat ska säkerställa att varje tillsynsmyndighet väljer och förfogar över egen personal, som ska ta instruktioner uteslutande från den berörda tillsynsmyndighetens ledamot eller ledamöter.

6. Varje medlemsstat ska säkerställa att varje tillsynsmyndighet blir föremål för finansiell kontroll, utan att detta påverkar tillsynsmyndighetens oberoende och att de förfogar över en separat, offentlig årsbudget som kan ingå i den övergripande statsbudgeten eller nationella budgeten.

Artikel 53

Allmänna villkor för tillsynsmyndighetens ledamöter

1. Medlemsstaterna ska föreskriva att varje ledamot av deras tillsynsmyndigheter ska utnämnas genom ett genom ett öppet förfarande med insyn av

— deras parlament,

— deras regering,

— deras statschef, eller

— ett oberoende organ som genom medlemsstatens nationella rätt anförtrotts utnämningen.

2. Varje ledamot ska ha de kvalifikationer, den erfarenhet och den kompetens, särskilt på området skydd av personuppgifter, som krävs för att ledamoten ska kunna utföra sitt uppdrag och utöva sina befogenheter.

3. En ledamots uppdrag ska upphöra då mandattiden löper ut eller om ledamoten avgår eller avsätts från sin tjänst i enlighet med den berörda medlemsstatens nationella rätt.

4. En ledamot får avsättas endast på grund av grov försummelse eller när ledamoten inte längre uppfyller de villkor som krävs för att utföra uppdraget.

Artikel 54

Regler för inrättandet av en tillsynsmyndighet

1. Varje medlemsstat ska fastställa följande i lag:

a) Varje tillsynsmyndighets inrättande.

b) De kvalifikationer och de villkor för lämplighet som krävs för att någon ska kunna utnämnas till ledamot av en tillsynsmyndighet.

c) Regler och förfaranden för att utse varje tillsynsmyndighets ledamot eller ledamöter.

d) Mandattiden för varje tillsynsmyndighets ledamot eller ledamöter, vilken inte får understiga fyra år, utom vid tillsättandet av de första ledamöterna efter den 24 maj 2016, då ett stegvis tillsättningsförfarande med kortare perioder för några av ledamöterna får tillämpas om detta är nödvändigt för att säkerställa myndighetens oberoende.

e) Huruvida varje tillsynsmyndighets ledamot eller ledamöter får ges förnyat mandat, och om så är fallet, för hur många perioder.

f) Vilka villkor som gäller för de skyldigheter som varje tillsynsmyndighets ledamot eller ledamöter och personal har, förbud mot handlingar, yrkesverksamhet och förmåner som står i strid därmed under och efter mandattiden och vilka bestämmelser som gäller för anställningens upphörande.

2. Varje tillsynsmyndighets ledamot eller ledamöter och personal ska i enlighet med unionsrätten eller medlemsstaternas nationella rätt omfattas av tystnadsplikt både under och efter sin mandattid vad avser konfidentiell information som de fått kunskap om under utförandet av deras uppgifter eller utövandet av deras befogenheter. Under mandatperioden ska denna tystnadsplikt i synnerhet gälla rapportering från fysiska personer om överträdelser av denna förordning.

Avsnitt 2

Behörighet, uppgifter och befogenheter

Artikel 55

Behörighet

1. Varje tillsynsmyndighet ska vara behörig att utföra de uppgifter och utöva de befogenheter som tilldelas den enligt denna förordning inom sin egen medlemsstats territorium.

2. Om behandling utförs av myndigheter eller privata organ som agerar på grundval av artikel 6.1 c eller e ska tillsynsmyndigheten i den berörda medlemsstaten vara behörig. I sådana fall ska artikel 56 inte tillämpas.

3. Tillsynsmyndigheterna ska inte vara behöriga att utöva tillsyn över domstolar som behandlar personuppgifter i sin dömande verksamhet.

Artikel 56

Den ansvariga tillsynsmyndighetens behörighet

1. Utan att det påverkar tillämpningen av artikel 55 ska tillsynsmyndigheten för den personuppgiftsansvariges eller personuppgiftsbiträdets huvudsakliga verksamhetsställe eller enda verksamhetsställe vara behörig att agera som ansvarig tillsynsmyndighet för den personuppgiftsansvariges eller personuppgiftsbiträdets gränsöverskridande behandling i enlighet med det förfarande som föreskrivs i artikel 60.

2. Genom undantag från punkt 1 ska varje tillsynsmyndighet vara behörig att behandla ett klagomål som lämnats in till denna eller en eventuell överträdelse av denna förordning, om sakfrågan i ärendet endast rör ett verksamhetsställe i medlemsstaten eller i väsentlig grad påverkar registrerade endast i medlemsstaten.

3. I de fall som avses i punkt 2 i den här artikeln ska tillsynsmyndigheten utan dröjsmål informera den ansvariga tillsynsmyndigheten om detta ärende. Inom tre veckor från det att den underrättats ska den ansvariga tillsynsmyndigheten besluta huruvida den kommer att behandla ärendet i enlighet med det förfarande som föreskrivs i artikel 60, med hänsyn till huruvida den personuppgiftsansvarige eller personuppgiftsbiträdet har eller inte har ett verksamhetsställe som är beläget i den medlemsstat där den tillsynsmyndighet som lämnat informationen är belägen.

4. Om den ansvariga tillsynsmyndigheten beslutar att behandla ärendet ska det ske i enlighet med det förfarande som föreskrivs i artikel 60. Den tillsynsmyndighet som underrättade den ansvariga tillsynsmyndigheten får lämna in ett utkast till beslut till den ansvariga tillsynsmyndigheten. Den ansvariga tillsynsmyndigheten ska ta största möjliga hänsyn till detta utkast till beslut när det utarbetar det utkast till beslut som avses i artikel 60.3.

5. Om den ansvariga tillsynsmyndigheten beslutar att inte behandla ärendet ska den tillsynsmyndighet som underrättade den ansvariga tillsynsmyndigheten behandla ärendet i enlighet med artiklarna 61 och 62.

6. Den ansvariga tillsynsmyndigheten ska vara den personuppgiftsansvariges eller personuppgiftsbiträdets enda motpart när det gäller den registreringsansvariges eller den personuppgiftsbiträdets gränsöverskridande behandling.

Artikel 57

Uppgifter

1. Utan att det påverkar de andra uppgifter som föreskrivs i denna förordning ska varje tillsynsmyndighet på sitt territorium ansvara för följande:

a) Övervaka och verkställa tillämpningen av denna förordning.

b) Öka allmänhetens medvetenhet om och förståelse för risker, regler, skyddsåtgärder och rättigheter i fråga om behandling. Särskild uppmärksamhet ska ägnas åt insatser som riktar sig till barn.

c) I enlighet med medlemsstatens nationella rätt ge rådgivning åt det nationella parlamentet, regeringen och andra institutioner och organ om lagstiftningsåtgärder och administrativa åtgärder rörande skyddet av fysiska personers rättigheter och friheter när det gäller behandling.

d) Öka personuppgiftsansvarigas och personuppgiftsbiträdens medvetenhet om sina skyldigheter enligt denna förordning.

e) På begäran tillhandahålla information till registrerade om hur de ska utöva sina rättigheter enligt denna förordning, och om så krävs samarbeta med tillsynsmyndigheter i andra medlemsstater för detta ändamål.

f) Behandla klagomål från en registrerad eller från ett organ, en organisation eller en sammanslutning enligt artikel 80, och där så är lämpligt undersöka den sakfråga som klagomålet gäller och inom rimlig tid underrätta den enskilde om hur undersökningen fortskrider och om resultatet, i synnerhet om det krävs ytterligare undersökningar eller samordning med en annan tillsynsmyndighet.

g) Samarbeta, inbegripet utbyta information, med och ge ömsesidigt bistånd till andra tillsynsmyndigheter för att se till att denna förordning tillämpas och verkställs på ett enhetligt sätt.

h) Utföra undersökningar om tillämpningen av denna förordning, inbegripet på grundval av information som erhålls från en annan tillsynsmyndighet eller annan myndighet.

i) Följa sådan utveckling som påverkar skyddet av personuppgifter, bland annat inom informations- och kommunikationsteknik och affärspraxis.

j) Anta sådana standardavtalsklausuler som avses i artiklarna 28.8 och 46.2 d.

k) Upprätta och föra en förteckning när det gäller kravet på en konsekvensbedömning avseende dataskydd enligt artikel 35.4.

l) Ge råd om behandling av personuppgifter enligt artikel 36.2.

m) Främja framtagande av uppförandekoder enligt artikel 40.1 samt yttra sig över och godkänna sådana uppförandekoder som tillhandahåller tillräckliga garantier, i enlighet med artikel 40.5.

n) Uppmuntra till inrättandet av certifieringsmekanismer för dataskydd och av sigill och märkningar för dataskydd i enlighet med artikel 42.1 samt godkänna certifieringskriterierna i enlighet med artikel 42.5.

o) I tillämpliga fall genomföra en periodisk översyn av certifieringar som utfärdats i enlighet med artikel 42.7.

p) Utarbeta och offentliggöra kriterier för ackreditering av ett organ för övervakning av uppförandekoder enligt artikel 41 och ett certifieringsorgan enligt artikel 43.

q) Ackreditera ett organ för övervakning av uppförandekoder enligt artikel 41 och ett certifieringsorgan enligt artikel 43.

r) Godkänna sådana avtalsklausuler och bestämmelser som avses i artikel 46.3.

s) Godkänna sådana bindande företagsbestämmelser som avses i artikel 47.

t) Bidra till styrelsens verksamhet.

u) Hålla arkiv över överträdelser av denna förordning och åtgärder som vidtagits i enlighet med artikel 58.2.

v) Utföra eventuella andra uppgifter som rör skyddet av personuppgifter.

2. Varje tillsynsmyndighet ska underlätta inlämningen av klagomål enligt punkt 1 f genom åtgärder såsom ett särskilt formulär för ändamålet, vilket också kan fyllas i elektroniskt, utan att andra kommunikationsformer utesluts.

3. Utförandet av alla tillsynsmyndigheters uppgifter ska vara avgiftsfritt för den registrerade och, i tillämpliga fall, för dataskyddsombudet.

4. Om en begäran är uppenbart ogrundad eller orimlig, särskilt på grund av dess repetitiva karaktär, får tillsynsmyndigheten ta ut en rimlig avgift grundad på de administrativa kostnaderna eller vägra att tillmötesgå begäran. Det åligger tillsynsmyndigheten att visa att begäran är uppenbart ogrundad eller orimlig.

Artikel 58

Befogenheter

1. Varje tillsynsmyndighet ska ha samtliga följande utredningsbefogenheter

a) Beordra den personuppgiftsansvarige eller personuppgiftsbiträdet, och i tillämpliga fall den personuppgiftsansvariges eller personuppgiftsbiträdets företrädare, att lämna all information som myndigheten behöver för att kunna fullgöra sina uppgifter.

b) Genomföra undersökningar i form av dataskyddstillsyn.

c) Genomföra en översyn av certifieringar som utfärdats i enlighet med artikel 42.7.

d) Meddela den personuppgiftsansvarige eller personuppgiftsbiträdet om en påstådd överträdelse av denna förordning.

e) Från den personuppgiftsansvarige och personuppgiftsbiträdet få tillgång till alla personuppgifter och all information som tillsynsmyndigheten behöver för att kunna fullgöra sina uppgifter.

f) Få tillträde till alla lokaler som tillhör den personuppgiftsansvarige och personuppgiftsbiträdet, inbegripet tillgång till all utrustning och alla andra medel för behandling av personuppgifter i överensstämmelse med unionens processrätt eller medlemsstaternas nationella processrätt.

2. Varje tillsynsmyndighet ska ha samtliga följande korrigerande befogenheter

a) Utfärda varningar till en personuppgiftsansvarig eller personuppgiftsbiträdet om att planerade behandlingar sannolikt kommer att bryta mot bestämmelserna i denna förordning.

b) Utfärda reprimander till en personuppgiftsansvarig eller personuppgiftsbiträdet om behandling bryter mot bestämmelserna i denna förordning.

c) Förelägga den personuppgiftsansvarige eller personuppgiftsbiträdet att tillmötesgå den registrerades begäran att få utöva sina rättigheter enligt denna förordning.

d) Förelägga en personuppgiftsansvarig eller ett personuppgiftsbiträde att se till att behandlingen sker i enlighet med bestämmelserna i denna förordning och om så krävs på ett specifikt sätt och inom en specifik period,

e) Förelägga den personuppgiftsansvarige att meddela den registrerade att en personuppgiftsincident har inträffat.

f) Införa en tillfällig eller definitiv begränsning av, inklusive ett förbud mot, behandling.

g) Förelägga om rättelse eller radering av personuppgifter samt begränsning av behandling enligt artiklarna 16, 17 och 18 och underrätta mottagare till vilka personuppgifterna har lämnats ut om dessa åtgärder enligt artiklarna 17.2 och 19.

h) Återkalla en certifiering eller beordra certifieringsorganet att återkalla en certifiering som utfärdats enligt artikel 42 eller 43, eller beordra certifieringsorganet att inte utfärda certifiering om kraven för certifiering inte eller inte längre uppfylls.

i) Påföra administrativa sanktionsavgifter i enlighet med artikel 83 utöver eller i stället för de åtgärder som avses i detta stycke, beroende på omständigheterna i varje enskilt fall.

j) Förelägga om att flödet av uppgifter till en mottagare i tredje land eller en internationell organisation ska avbrytas.

3. Varje tillsynsmyndighet ska ha samtliga följande befogenheter att utfärda tillstånd och att ge råd:

a) Ge råd till den personuppgiftsansvarige i enlighet med det förfarande för förhandssamråd som avses i artikel 36.

b) På eget initiativ eller på begäran avge yttranden till det nationella parlamentet, medlemsstatens regering eller, i enlighet med medlemsstatens nationella rätt, till andra institutioner och organ samt till allmänheten, i frågor som rör skydd av personuppgifter.

c) Ge tillstånd till behandling enligt artikel 36.5 om medlemsstatens rätt kräver ett sådant förhandstillstånd.

d) Avge ett yttrande om och godkänna utkast till uppförandekoder enligt artikel 40.5.

e) Ackreditera certifieringsorgan i enlighet med artikel 43.

f) Utfärda certifieringar och godkänna kriterier för certifiering i enlighet med artikel 42.5.

g) Anta standardiserade dataskyddsbestämmelser enligt artiklarna 28.8 och 46.2 d.

h) Godkänna avtalsklausuler enligt artikel 46.3 a.

i) Godkänna administrativa överenskommelser enligt artikel 46.3 b.

j) Godkänna bindande företagsbestämmelser enligt artikel 47.

4. Utövandet av de befogenheter som tillsynsmyndigheten tilldelas enligt denna artikel ska omfattas av lämpliga skyddsåtgärder, inbegripet effektiva rättsmedel och rättssäkerhet, som fastställs i unionsrätten och i medlemsstaternas nationella rätt i enlighet med stadgan.

5. Varje medlemsstat ska i lagstiftning fastställa att dess tillsynsmyndighet ska ha befogenhet att upplysa de rättsliga myndigheterna om överträdelser av denna förordning och vid behov att inleda eller på övrigt vis delta i rättsliga förfaranden, för att verkställa bestämmelserna i denna förordning.

6. Varje medlemsstat får i lagstiftning föreskriva att dess tillsynsmyndighet ska ha ytterligare befogenheter utöver dem som avses i punkterna 1, 2 och 3. Utövandet av dessa befogenheter ska inte påverka den effektiva tillämpningen av kapitel VII.

Artikel 59

Verksamhetsrapporter

Varje tillsynsmyndighet ska upprätta en årlig rapport om sin verksamhet, vilken kan omfatta en förteckning över typer av anmälda överträdelser och typer av åtgärder som vidtagits i enlighet med artikel 58.2. Rapporterna ska översändas till det nationella parlamentet, regeringen och andra myndigheter som utsetts genom medlemsstatens nationella rätt. De ska göras tillgängliga för allmänheten, kommissionen och styrelsen.

KAPITEL VII

Samarbete och enhetlighet

Avsnitt 1

Samarbete

Artikel 60

Samarbete mellan den ansvariga tillsynsmyndigheten och de andra berörda tillsynsmyndigheterna

1. Den ansvariga tillsynsmyndigheten ska samarbeta med de andra berörda tillsynsmyndigheterna i enlighet med denna artikel i en strävan att uppnå samförstånd. Den ansvariga tillsynsmyndigheten och de berörda tillsynsmyndigheterna ska utbyta all relevant information med varandra.

2. Den ansvariga tillsynsmyndigheten får när som helst begära att andra berörda tillsynsmyndigheter ger ömsesidigt bistånd i enlighet med artikel 61 och får genomföra gemensamma insatser i enlighet med artikel 62, i synnerhet för att utföra utredningar eller övervaka genomförandet av en åtgärd som avser en personuppgiftsansvarig eller ett personuppgiftsbiträde som är etablerad i en annan medlemsstat.

3. Den ansvariga tillsynsmyndigheten ska utan dröjsmål meddela de andra berörda tillsynsmyndigheterna den relevanta informationen i ärendet. Den ska utan dröjsmål lägga fram ett utkast till beslut för de andra berörda tillsynsmyndigheterna så att de kan avge ett yttrande och ta vederbörlig hänsyn till deras synpunkter.

4. Om någon av de andra berörda tillsynsmyndigheterna inom en period av fyra veckor efter att de har rådfrågats i enlighet med punkt 3 i den här artikeln uttrycker en relevant och motiverad invändning mot utkastet till beslut ska den ansvariga tillsynsmyndigheten, om den inte instämmer i den relevanta och motiverade invändningen eller anser att invändningen inte är relevant eller motiverad, överlämna ärendet till den mekanism för enhetlighet som avses i artikel 63.

5. Om den ansvariga tillsynsmyndigheten avser att följa den relevanta och motiverade invändningen ska den till de andra berörda tillsynsmyndigheterna överlämna ett reviderat utkast till beslut så att de kan avge ett yttrande. Detta reviderade utkast till beslut ska omfattas av det förfarande som avses i punkt 4 inom en period av två veckor.

6. Om ingen av de andra berörda tillsynsmyndigheterna har gjort invändningar mot det utkast till beslut som den ansvariga tillsynsmyndigheten har lagt fram inom den period som avses i punkterna 4 och 5 ska den ansvariga tillsynsmyndigheten och de berörda tillsynsmyndigheterna anses samtycka till detta utkast till beslut och ska vara bundna av det.

7. Den ansvariga tillsynsmyndigheten ska anta och meddela beslutet till den personuppgiftsansvariges eller personuppgiftsbiträdets huvudsakliga eller enda verksamhetsställe, allt efter omständigheterna, och underrätta de andra berörda tillsynsmyndigheterna och styrelsen om beslutet i fråga, inbegripet en sammanfattning av relevanta fakta och en relevant motivering. Den tillsynsmyndighet till vilken ett klagomål har lämnats in ska underrätta den enskilde om beslutet.

8. Om ett klagomål avvisas eller avslås ska den tillsynsmyndighet till vilken klagomålet lämnades in, genom undantag från punkt 7, anta beslutet och meddela den enskilde samt informera den personuppgiftsansvarige.

9. Om den ansvariga tillsynsmyndigheten och de berörda tillsynsmyndigheterna är överens om att avvisa eller avslå delar av ett klagomål och att vidta åtgärder beträffande andra delar av klagomålet ska ett separat beslut antas för var och en av dessa delar av frågan. Den ansvariga tillsynsmyndigheten ska anta beslutet om den del som gäller åtgärder som avser den personuppgiftsansvarige och meddela det till den personuppgiftsansvariges eller personuppgiftsbiträdets huvudsakliga eller enda verksamhetsställe på medlemsstatens territorium och underrätta den enskilde om detta, medan den enskildes tillsynsmyndighet ska anta beslutet för den del som gäller avvisande av eller avslag på klagomålet och meddela det till den enskilde och underrätta den personuppgiftsansvarige eller personuppgiftsbiträdet om detta.

10. Efter att den personuppgiftsansvarige eller personuppgiftsbiträdet har meddelats om den ansvariga myndighetens beslut i enlighet med punkterna 7 och 9 ska den personuppgiftsansvarige eller personuppgiftsbiträdet vidta nödvändiga åtgärder för att se till att beslutet efterlevs vad gäller behandling med koppling till alla deras verksamhetsställen i unionen. Den personuppgiftsansvarige eller personuppgiftsbiträdet ska meddela den ansvariga tillsynsmyndigheten vilka åtgärder som har vidtagits för att efterleva beslutet, och den ansvariga tillsynsmyndigheten ska informera de andra berörda tillsynsmyndigheterna.

11. Om en berörd tillsynsmyndighet under exceptionella omständigheter har skäl att anse att det finns ett brådskande behov av att agera för att skydda registrerades intressen ska det skyndsamma förfarande som avses i artikel 66 tillämpas.

12. Den ansvariga tillsynsmyndigheten och de andra berörda tillsynsmyndigheterna ska förse varandra med den information som krävs enligt denna artikel på elektronisk väg med användning av ett standardiserat format.

Artikel 61

Ömsesidigt bistånd

1. Tillsynsmyndigheterna ska utbyta relevant information och ge ömsesidigt bistånd i arbetet för att genomföra och tillämpa denna förordning på ett enhetligt sätt, och ska införa åtgärder som bidrar till ett verkningsfullt samarbete. Det ömsesidiga biståndet ska i synnerhet omfatta begäranden om information och tillsynsåtgärder, till exempel begäranden om utförande av förhandstillstånd och förhandssamråd, inspektioner och utredningar.

2. Varje tillsynsmyndighet ska vidta lämpliga åtgärder som krävs för att besvara en begäran från en annan tillsynsmyndighet utan onödigt dröjsmål och inte senare än en månad efter det att den tagit emot begäran. Till sådana åtgärder hör bland annat att översända relevant information om genomförandet av en pågående utredning.

3. En begäran om bistånd ska innehålla all nödvändig information, inklusive syftet med begäran och skälen till denna. Information som utbytts får endast användas för det syfte för vilket den har begärts.

4. Den tillsynsmyndighet som tar emot en begäran får endast vägra att tillmötesgå begäran om

a) den inte är behörig att behandla den sakfråga som begäran avser eller de åtgärder som det begärs att den ska utföra, eller

b) det skulle stå i strid med denna förordning eller unionsrätten eller den nationella rätt i en medlemsstat som tillsynsmyndigheten omfattas av att tillmötesgå begäran.

5. Den tillsynsmyndighet som tagit emot begäran ska meddela den myndighet som begäran kommer ifrån om resultatet eller, allt efter omständigheterna, om hur de åtgärder som vidtagits för att tillmötesgå begäran fortskrider. Den tillsynsmyndighet som tagit emot begäran ska redogöra för sina skäl för att vägra tillmötesgå begäran i enlighet med punkt 4.

6. Den tillsynsmyndighet som tar emot en begäran ska som regel tillhandahålla den information som begärts av andra tillsynsmyndigheter på elektronisk väg med användning av ett standardiserat format.

7. Tillsynsmyndigheter som tar emot en begäran får inte ta ut någon avgift för åtgärder som vidtagits av dem till följd av en begäran om ömsesidigt bistånd. Tillsynsmyndigheter får i undantagsfall komma överens med andra tillsynsmyndigheter om regler för ersättning från varandra för vissa utgifter i samband med tillhandahållande av ömsesidigt bistånd.

8. Om en tillsynsmyndighet inte tillhandahåller den information som avses i punkt 5 i denna artikel inom en månad efter det att den erhållit begäran från en annan tillsynsmyndighet får den begärande myndigheten anta en provisorisk åtgärd på sin medlemsstats territorium i enlighet med artikel 55.1. I detta fall ska det brådskande behov av att agera enligt artikel 66.1 anses vara uppfyllt och kräva ett brådskande bindande beslut från styrelsen i enlighet med artikel 66.2.

9. Kommissionen får genom genomförandeakter närmare ange format och förfaranden för sådant ömsesidigt bistånd som avses i denna artikel samt formerna för elektronisk överföring av information tillsynsmyndigheter emellan, samt mellan tillsynsmyndigheter och styrelsen, i synnerhet det standardiserade format som avses i punkt 6 i den här artikeln. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 93.2.

Artikel 62

Tillsynsmyndigheters gemensamma insatser

1. Tillsynsmyndigheter ska vid behov genomföra gemensamma insatser, inbegripet gemensamma utredningar och gemensamma verkställighetsåtgärder i vilka ledamöter eller personal från andra medlemsstaters tillsynsmyndigheter deltar.

2. Om den personuppgiftsansvarige eller personuppgiftsbiträdet har verksamhetsställen i flera medlemsstater eller om ett betydande antal registrerade personer i mer än en medlemsstat sannolikt kommer att påverkas i väsentlig grad av att uppgifter behandlas, ska tillsynsmyndigheterna i var och en av dessa medlemsstater ha rätt att delta i de gemensamma insatserna. Den tillsynsmyndighet som är behörig enligt artikel 56.1 eller 56.4 ska bjuda in tillsynsmyndigheterna i var och en av de berörda medlemsstaterna att delta i de gemensamma insatserna och ska utan dröjsmål svara på en annan tillsynsmyndighets begäran att få delta.

3. En tillsynsmyndighet får, i enlighet med medlemsstatens nationella rätt och efter godkännande från ursprungslandets tillsynsmyndighet, tilldela befogenheter, inklusive utredningsbefogenheter, till ledamöter eller personal från ursprungslandets tillsynsmyndighet som deltar i gemensamma insatser eller, i den mån lagstiftningen i den medlemsstat som är värdland för tillsynsmyndigheten tillåter detta, medge att ursprungslandets tillsynsmyndighets ledamöter eller personal utövar utredningsbefogenheter enligt lagstiftningen i ursprungslandets tillsynsmyndighets medlemsstat. Sådana utredningsbefogenheter får endast utövas under vägledning och i närvaro av ledamöter eller personal från värdlandets tillsynsmyndighet. Ledamöter och personal från ursprungslandets tillsynsmyndighet ska omfattas av den medlemsstats nationella rätt som gäller för värdlandets tillsynsmyndighet.

4. Om personal från ursprungslandets tillsynsmyndighet verkar i en annan medlemsstat i enlighet med punkt 1 ska värdtillsynsmyndighetens medlemsstat ansvara för deras handlingar, vilket inbegriper ansvar för skador som personalen vållar i samband med insatserna, i enlighet med rätten i den medlemsstat på vars territorium personalen verkar.

5. Den medlemsstat på vars territorium skadorna förorsakades ska ersätta sådana skador enligt de villkor som gäller för skador som förorsakas av dess egen personal. Den medlemsstat vars tillsynsmyndighets tjänstemän har orsakat en person skada på någon annan medlemsstats territorium ska fullt ut ersätta den andra medlemsstaten för det belopp som denna har betalat ut till den personens rättsinnehavare.

6. Utan att det påverkar rättigheterna gentemot tredje man och tillämpningen av punkt 5, ska varje medlemsstat i de fall som nämns i punkt 1 avstå från att kräva ersättning från en annan medlemsstat för skador som avses i punkt 4.

7. Om en gemensam insats planeras och en tillsynsmyndighet inte inom en månad har uppfyllt sin skyldighet enligt punkt 2 i den här artikeln, andra meningen får övriga tillsynsmyndigheter anta provisoriska åtgärder på sina respektive medlemsstaters territorium i enlighet med artikel 55. I detta fall ska det brådskande behov av att agera enligt artikel 66.1 anses vara uppfyllt och kräva ett yttrande eller ett brådskande bindande beslut från styrelsen i enlighet med artikel 66.2.

Avsnitt 2

Enhetlighet

Artikel 63

Mekanism för enhetlighet

För att bidra till en enhetlig tillämpning av denna förordning i hela unionen ska tillsynsmyndigheterna samarbeta med varandra och, i förekommande fall, med kommissionen, genom den mekanism för enhetlighet som föreskrivs i detta avsnitt.

Artikel 64

Yttrande från Styrelsen

1. Styrelsen ska avge ett yttrande när en behörig tillsynsmyndighet avser att anta någon av åtgärderna nedan. I detta syfte ska den behöriga tillsynsmyndigheten skicka utkastet till beslut till styrelsen när det

a) syftar till att anta en förteckning över behandling som omfattas av kravet på en konsekvensbedömning avseende dataskydd enligt artikel 35.4,

b) rör ett ärende i enlighet med artikel 40.7 om huruvida ett utkast till uppförandekoder eller en ändring eller förlängning av en uppförandekod är förenlig med denna förordning,

c) syftar till att godkänna kriterierna för ackreditering av ett organ enligt artikel 41.3 eller ett certifieringsorgan enligt artikel 43.3,

d) syftar till att fastställa standardiserade dataskyddsbestämmelser enligt artiklarna 46.2 d och 28.8,

e) syftar till att godkänna sådana avtalsklausuler som avses i artikel 46.3 a, eller

f) syftar till att godkänna bindande företagsbestämmelser enligt artikel 47.

2. Varje tillsynsmyndighet, styrelsens ordförande eller kommissionen får i syfte att erhålla ett yttrande begära att styrelsen granskar en fråga med allmän räckvidd eller som har följder i mer än en medlemsstat, i synnerhet om en behörig myndighet inte uppfyller sina skyldigheter i fråga om ömsesidigt bistånd i enlighet med artikel 61 eller i fråga om gemensamma insatser i enlighet med artikel 62.

3. I de fall som avses i punkterna 1 och 2 ska styrelsen avge ett yttrande i den fråga som ingivits till den, förutsatt att den inte redan har avgett ett yttrande i samma fråga. Detta yttrande ska antas med enkel majoritet av styrelsens ledamöter inom åtta veckor. Denna period får förlängas med ytterligare sex veckor med hänsyn till sakfrågans komplexitet. Vad gäller det utkast till beslut som avses i punkt 1 som spridits till styrelsens ledamöter i enlighet med punkt 5, ska en ledamot som inte har gjort invändningar inom en rimlig period som ordföranden angett anses samtycka till utkastet till beslut.

4. Tillsynsmyndigheterna och kommissionen ska utan onödigt dröjsmål i ett standardiserat elektroniskt format till styrelsen översända all relevant information, som allt efter omständigheterna får utgöras av en sammanfattning av sakförhållanden, utkastet till beslut, grunden till att en sådan åtgärd är nödvändig och synpunkter från övriga berörda tillsynsmyndigheter.

5. Styrelsens ordförande ska utan onödigt dröjsmål och på elektronisk väg upplysa

a) styrelsens ledamöter samt kommissionen om all relevant information som meddelats styrelsen i ett standardiserat format; styrelsens sekretariat ska vid behov tillhandahålla översättningar av relevant information; och

b) den tillsynsmyndighet som, allt efter omständigheterna, avses i punkterna 1 och 2 samt kommissionen om yttrandet, och ska också offentliggöra det.

6. Den behöriga tillsynsmyndigheten får inte anta sitt utkast till beslut enligt punkt 1 inom den period som avses i punkt 3.

7. Den tillsynsmyndighet som avses i punkt 1 ska ta största möjliga hänsyn till styrelsens yttrande och ska, inom två veckor efter att yttrandet inkommit, i ett standardiserat elektroniskt format meddela styrelsens ordförande om huruvida den kommer att hålla fast vid eller ändra sitt utkast till beslut, och i förekommande fall översända det ändrade utkastet till beslut.

8. Om den berörda tillsynsmyndigheten underrättar styrelsens ordförande inom den period som avses i punkt 7 i den här artikeln om att den inte avser att följa styrelsens yttrande, helt eller delvis, och tillhandahåller en relevant motivering, ska artikel 65.1 tillämpas.

Artikel 65

Tvistlösning genom styrelsen

1. För att säkerställa en korrekt och enhetlig tillämpning av denna förordning i enskilda fall ska styrelsen anta ett bindande beslut i följande fall:

a) Om en berörd tillsynsmyndighet i ett fall som avses i artikel 60.4 har gjort en relevant och motiverad invändning mot ett utkast till beslut av den ansvariga myndigheten, eller om den ansvariga myndigheten har avslagit denna invändning med motiveringen att den inte var relevant eller motiverad. Det bindande beslutet ska avse alla ärenden som är föremål för den relevanta och motiverade invändningen, särskilt frågan om huruvida det föreligger en överträdelse av denna förordning.

b) Om det finns motstridiga åsikter om vilken av de berörda tillsynsmyndigheterna som är behörig för det huvudsakliga verksamhetsstället.

c) Om en behörig tillsynsmyndighet inte begär ett yttrande från styrelsen i de fall som avses i artikel 64.1, eller inte följer ett yttrande som styrelsen avger enligt artikel 64. I detta fall får varje berörd tillsynsmyndighet eller kommissionen översända ärendet till styrelsen.

2. Det beslut som avses i punkt 1 ska antas inom en månad efter det att sakfrågan hänskjutits med två tredjedels majoritet av styrelsens ledamöter. Denna period får förlängas med ytterligare en månad med hänsyn till sakfrågans komplexitet. Det beslut som avses i punkt 1 ska vara motiverat och riktat till den ansvariga tillsynsmyndigheten och alla berörda tillsynsmyndigheter och ska vara bindande för dem.

3. Om styrelsen inte har kunnat anta något beslut inom de perioder som avses i punkt 2 ska den anta sitt beslut inom två veckor efter utgången av den andra månad som avses i punkt 2 med enkel majoritet av styrelsens ledamöter. Om styrelsens ledamöter är delade i frågan ska beslutet antas i enlighet med ordförandens röst.

4. De berörda tillsynsmyndigheterna ska inte anta något beslut om den sakfråga som ingivits till styrelsen i enlighet med punkt 1 under de perioder som avses i punkterna 2 och 3.

5. Styrelsens ordförande ska utan onödigt dröjsmål meddela de berörda tillsynsmyndigheterna det beslut som avses i punkt 1. Kommissionen ska informeras om detta. Beslutet ska utan dröjsmål offentliggöras på styrelsens webbplats efter att tillsynsmyndigheten har meddelat det slutliga beslut som avses i punkt 6.

6. Den ansvariga tillsynsmyndigheten eller, allt efter omständigheterna, den tillsynsmyndighet till vilken klagomålet har ingetts ska anta sitt slutliga beslut på grundval av det beslut som avses i punkt 1 i den här artikeln, utan onödigt dröjsmål och senast en månad efter det att styrelsen har meddelat sitt beslut. Den ansvariga tillsynsmyndigheten eller, allt efter omständigheterna, den tillsynsmyndighet till vilken klagomålet har ingetts ska underrätta styrelsen om vilken dag dess slutliga beslut meddelas till den personuppgiftsansvarige respektive personuppgiftsbiträdet och den registrerade. De berörda tillsynsmyndigheternas slutliga beslut ska antas i enlighet med bestämmelserna i artikel 60.7, 60.8 och 60.9. Det slutliga beslutet ska hänvisa till det beslut som avses i punkt 1 i den här artikeln och ska precisera att det beslut som avses i punkt 1 kommer att offentliggöras på styrelsens webbplats i enlighet med punkt 5 i den här artikeln. Det beslut som avses i punkt 1 i den här artikeln ska fogas till det slutliga beslutet.

Artikel 66

Skyndsamt förfarande

1. Under exceptionella omständigheter får en berörd tillsynsmyndighet med avvikelse från den mekanism för enhetlighet som avses i artiklarna 63, 64 och 65 eller det förfarande som avses i artikel 60 omedelbart vidta provisoriska åtgärder avsedda att ha rättsverkan på det egna territoriet och med förutbestämd varaktighet som inte överskrider tre månader, om den anser att det finns ett brådskande behov av att agera för att skydda registrerades rättigheter och friheter. Tillsynsmyndigheten ska utan dröjsmål underrätta de andra berörda tillsynsmyndigheterna, styrelsen och kommissionen om dessa åtgärder och om skälen till att de vidtas.

2. Om en tillsynsmyndighet har vidtagit en åtgärd enligt punkt 1 och anser att definitiva åtgärder skyndsamt måste antas, får den begära ett brådskande yttrande eller ett brådskande bindande beslut från styrelsen; den ska då motivera varför den begär ett sådant yttrande eller beslut.

3. Om en behörig tillsynsmyndighet inte har vidtagit någon lämplig åtgärd i en situation som kräver skyndsam handling för att skydda registrerades rättigheter och friheter, får vilken tillsynsmyndighet som helst begära ett brådskande yttrande eller, i tillämpliga fall, ett brådskande bindande beslut från styrelsen, varvid den ska motivera varför den begär ett sådant yttrande eller beslut och varför åtgärden måste vidtas skyndsamt.

4. Genom undantag från artiklarna 64.3 och 65.2 ska ett brådskande yttrande eller ett brådskande beslut enligt punkterna 2 och 3 i den här artikeln antas inom två veckor med enkel majoritet av styrelsens ledamöter.

Artikel 67

Utbyte av information

Kommissionen får anta genomförandeakter med allmän räckvidd i syfte att närmare ange tillvägagångssätten för elektroniskt utbyte av information mellan tillsynsmyndigheter samt mellan tillsynsmyndigheter och styrelsen, särskilt det standardiserade format som avses i artikel 64.

Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 93.2.

Avsnitt 3

Europeiska dataskyddsstyrelsen

Artikel 68

Europeiska dataskyddsstyrelsen

1. Europeiska dataskyddsstyrelsen (nedan kallad *styrelsen*) inrättas härmed som ett unionsorgan och ska ha ställning som juridisk person.

2. Styrelsen ska företrädas av sin ordförande.

3. Styrelsen ska bestå av chefen för en tillsynsmyndighet per medlemsstat och av Europeiska datatillsynsmannen eller deras respektive företrädare.

4. Om en medlemsstat har mer än en tillsynsmyndighet som ansvarar för att övervaka tillämpningen av bestämmelserna i denna förordning ska en gemensam företrädare utses i enlighet med den medlemsstatens nationella rätt.

5. Kommissionen ska ha rätt att delta i styrelsens verksamhet och möten utan rösträtt. Kommissionen ska utse en egen företrädare. Styrelsens ordförande ska underrätta kommissionen om styrelsens verksamhet.

6. I de fall som avses i artikel 65 ska Europeiska datatillsynsmannen endast ha rösträtt i fråga om beslut som rör principer och regler som är tillämpliga på unionens institutioner, organ och byråer, och som i allt väsentligt motsvarar dem i denna förordning.

Artikel 69

Oberoende

1. Styrelsen ska vara oberoende när den fullgör sina uppgifter eller utövar sina befogenheter i enlighet med artiklarna 70 och 71.

2. Utan att detta påverkar kommissionens rätt att lämna en begäran enligt artikel 70.1 b och 70.2 ska styrelsen när den fullgör sina uppgifter eller utövar sina befogenheter varken begära eller ta emot instruktioner av någon.

Artikel 70

Styrelsens uppgifter

1. Styrelsen ska se till att denna förordning tillämpas enhetligt. För detta ändamål ska styrelsen, på eget initiativ eller i förekommande fall på begäran av kommissionen, i synnerhet

a) övervaka och säkerställa korrekt tillämpning av denna förordning i de fall som avses i artiklarna 64 och 65 utan att det påverkar de nationella tillsynsmyndigheternas uppgifter,

b) ge kommissionen råd i alla frågor som gäller skydd av personuppgifter inom unionen, inklusive om eventuella förslag till ändring av denna förordning,

c) ge kommissionen råd om format och förfaranden för informationsutbyte mellan personuppgiftsansvariga, personuppgiftsbiträden och tillsynsmyndigheter för bindande företagsbestämmelser,

d) utfärda riktlinjer, rekommendationer och bästa praxis beträffande förfaranden för att radera länkar, kopior eller reproduktioner av personuppgifter från allmänt tillgängliga kommunikationstjänster enligt artikel 17.2,

e) på eget initiativ eller på begäran av en av sina ledamöter eller av kommissionen behandla frågor om tillämpningen av denna förordning och utfärda riktlinjer, rekommendationer och bästa praxis i syfte att främja en enhetlig tillämpning av denna förordning,

f) utfärda riktlinjer, rekommendationer och bästa praxis i enlighet med led e i denna punkt för att närmare ange kriterierna och villkoren för profileringsbaserade beslut enligt artikel 22.2,

g) utfärda riktlinjer, rekommendationer och bästa praxis i enlighet med led e i denna punkt för att konstatera sådana personuppgiftsincidenter och fastställa sådant onödigt dröjsmål som avses i artikel 33.1 och 33.2 och för de särskilda omständigheter under vilka en personuppgiftsansvarig eller ett personuppgiftsbiträde är skyldig att anmäla personuppgiftsincidenten,

h) utfärda riktlinjer, rekommendationer och bästa praxis i enlighet med led e i denna punkt angående de omständigheter under vilka en personuppgiftsincident sannolikt kommer att leda till hög risk för rättigheterna och friheterna för de fysiska personer som avses i artikel 34.1,

i) utfärda riktlinjer, rekommendationer och bästa praxis i enlighet med led e i denna punkt för att närmare ange kriterierna och kraven för överföringar av personuppgifter på grundval av bindande företagsbestämmelser som personuppgiftsansvariga eller personuppgiftsbiträden följer samt ytterligare nödvändiga krav för att säkerställa skyddet för personuppgifter för berörda registrerade enligt artikel 47,

j) utfärda riktlinjer, rekommendationer och bästa praxis i enlighet med led e i denna punkt för att närmare ange kriterierna och villkoren för överföring av personuppgifter på grundval av artikel 49.1,

k) utforma riktlinjer för tillsynsmyndigheterna i fråga om tillämpningen av de åtgärder som avses i artikel 58.1, 58.2 och 58.3 och fastställandet av administrativa sanktionsavgifter i enlighet med artikel 83,

l) se över den praktiska tillämpningen av de riktlinjer och rekommendationer samt den bästa praxis som avses i leden e och f,

m) utfärda riktlinjer, rekommendationer och bästa praxis i enlighet med led e i denna punkt för att fastställa gemensamma förfaranden för fysiska personers rapportering av överträdelser av denna förordning enligt artikel 54.2,

n) främja utarbetandet av uppförandekoder och införandet av certifieringsmekanismer för dataskydd och sigill och märkningar för dataskydd i enlighet med artiklarna 40 och 42,

o) ackreditera certifieringsorgan och utföra sin periodiska översyn i enlighet med artikel 43 och föra ett offentligt register över ackrediterade organ i enlighet med artikel 43.6 och över de ackrediterade personuppgiftsansvariga eller personuppgiftsbiträdena som är etablerade i tredjeländer i enlighet med artikel 42.7,

p) närmare ange de krav som avses i artikel 43.3 i syfte att ackreditera certifieringsorgan enligt artikel 42,

q) avge ett yttrande till kommissionen om de certifieringskrav som avses i artikel 43.8,

r) avge ett yttrande till kommissionen om de symboler som avses i artikel 12.7,

s) avge ett yttrande till kommissionen för bedömningen av adekvat skyddsnivå i ett tredjeland eller en internationell organisation, inklusive för bedömningen av huruvida ett tredjeland, ett territorium eller en eller flera specificerade sektorer inom det tredjelandet, eller en internationell organisation inte längre säkerställer en adekvat skyddsnivå; i detta syfte ska kommissionen lämna all nödvändig dokumentation till styrelsen, inklusive korrespondens med regeringen i tredjelandet, med avseende på tredjelandet, territoriet eller den specificerade sektorn, eller till databehandlingssektorn i tredjelandet eller den internationella organisationen,

t) avge yttranden om utkast till beslut som läggs fram av tillsynsmyndigheter inom den mekanism för enhetlighet som avses i artikel 64.1, i ärenden som ingivits i enlighet med artikel 64.2 och anta bindande beslut i enlighet med artikel 65, inbegripet de fall som avses i artikel 66,

u) främja samarbete och effektivt bilateralt och multilateralt utbyte av bästa praxis och information mellan tillsynsmyndigheterna,

v) främja gemensamma utbildningsprogram och underlätta personalutbyte mellan tillsynsmyndigheterna och där så är lämpligt även med tillsynsmyndigheter i tredjeländer eller internationella organisationer,

w) främja utbyte av kunskap och dokumentation om lagstiftning om och praxis för dataskydd med tillsynsmyndigheter för dataskydd i hela världen.

x) avge yttranden över de uppförandekoder som utarbetas på unionsnivå i enlighet med artikel 40.9, och

y) föra ett offentligt elektroniskt register över tillsynsmyndigheters beslut och domstolars avgöranden i frågor som hanteras inom mekanismen för enhetlighet.

2. När kommissionen begär rådgivning från styrelsen får den ange en tidsfrist med hänsyn till hur brådskande ärendet är.

3. Styrelsen ska vidarebefordra sina yttranden, riktlinjer, rekommendationer och bästa praxis till kommissionen och till den kommitté som avses i artikel 93, samt offentliggöra dem.

4. När så är lämpligt ska styrelsen samråda med berörda parter och ge dem möjlighet att yttra sig inom rimlig tid. styrelsen ska, utan att det påverkar tillämpningen av artikel 76, offentliggöra resultatet av samrådsförfarandet.

Artikel 71

Rapporter

1. Styrelsen ska sammanställa en årsrapport om skydd av fysiska personer vid behandling inom unionen och, i förekommande fall, i tredjeländer och internationella organisationer. Rapporten ska offentliggöras och översändas till Europaparlamentet, rådet och kommissionen.

2. Årsrapporten ska också innehålla en översikt över den praktiska tillämpningen av de riktlinjer och rekommendationer och den bästa praxis som avses i artikel 70.1 l liksom de bindande beslut som avses i artikel 65.

Artikel 72

Förfarande

1. Styrelsen ska fatta beslut med enkel majoritet av dess ledamöter, om inte annat anges i denna förordning.

2. Styrelsen ska själv anta sin arbetsordning med två tredjedels majoritet av sina ledamöter och fastställa sina arbetsformer.

Artikel 73

Ordförande

1. Styrelsen ska med enkel majoritet välja en ordförande och två vice ordförande bland sina ledamöter.

2. Ordförandens och de vice ordförandenas mandattid ska vara fem år och kunna förnyas en gång.

Artikel 74

Ordförandens uppgifter

1. Ordföranden ska ha i uppgift att

a) sammankalla till styrelsens möten och planera dagordningen,

b) meddela beslut som antas av styrelsen i enlighet med artikel 65 till den ansvariga tillsynsmyndigheten och de berörda tillsynsmyndigheterna,

c) se till att styrelsens uppgifter fullgörs i tid, särskilt i fråga om den mekanism för enhetlighet som avses i artikel 63.

2. Fördelningen av uppgifter mellan ordföranden och de vice ordförandena ska fastställas i styrelsens arbetsordning.

Artikel 75

Sekretariatet

1. Styrelsen ska förfoga över ett sekretariat som ska tillhandahållas av Europeiska datatillsynsmannen.

2. Sekretariatet ska utföra sina uppgifter enbart under ledning av ordföranden för styrelsen.

3. Den personal vid Europeiska datatillsynsmannen som utför de uppgifter som styrelsen tilldelas genom denna förordning ska följa separata rapporteringsvägar från den personal som utför de uppgifter som Europeiska datatillsynsmannen tilldelas.

4. När så är lämpligt ska styrelsen och Europeiska datatillsynsmannen fastställa och offentliggöra ett samförståndsavtal för genomförande av denna artikel, som fastställer villkoren för deras samarbete, och som ska tillämpas på den personal vid Europeiska datatillsynsmannen som utför de uppgifter som styrelsen tilldelas genom denna förordning.

5. Sekretariatet ska förse styrelsen med analysstöd samt administrativt och logistiskt stöd.

6. Sekretariatet ska särskilt ansvara för

a) styrelsens löpande arbete,

b) kommunikationen mellan styrelsens ledamöter, dess ordförande och kommissionen,

c) kommunikationen med andra institutioner och med allmänheten,

d) användningen av elektroniska medel för intern och extern kommunikation,

e) översättning av relevant information,

f) förberedelser och uppföljning av styrelsens möten,

g) förberedelse, sammanställning och offentliggörande av yttranden, beslut om lösning av tvister mellan tillsynsmyndigheter och andra texter som antas av styrelsen.

Artikel 76

Konfidentialitet

1. Styrelsens överläggningar ska vara konfidentiella i de fall som styrelsen bedömer detta vara nödvändigt, i enlighet med vad som anges i dess arbetsordning.

2. Tillgången till handlingar som skickas till styrelsens ledamöter, till experter eller till företrädare för tredje part ska regleras av Europaparlamentets och rådets förordning (EG) nr 1049/2001 ([1]).

KAPITEL VIII

Rättsmedel, ansvar och sanktioner

Artikel 77

Rätt att lämna in klagomål till en tillsynsmyndighet

1. Utan att det påverkar något annat administrativt prövningsförfarande eller rättsmedel, ska varje registrerad som anser att behandlingen av personuppgifter som avser henne eller honom strider mot denna förordning ha rätt att lämna in ett klagomål till en tillsynsmyndighet, särskilt i den medlemsstat där han eller hon har sin hemvist eller sin arbetsplats eller där det påstådda intrånget begicks.

2. Den tillsynsmyndighet till vilken klagomålet har ingetts ska underrätta den enskilde om hur arbetet med klagomålet fortskrider och vad resultatet blir, inbegripet möjligheten till rättslig prövning enligt artikel 78.

Artikel 78

Rätt till ett effektivt rättsmedel mot tillsynsmyndighetens beslut

1. Utan att det påverkar något annat administrativt prövningsförfarande eller prövningsförfarande utanför domstol ska varje fysisk eller juridisk person ha rätt till ett effektivt rättsmedel mot ett rättsligt bindande beslut rörande dem som meddelats av en tillsynsmyndighet.

2. Utan att det påverkar något annat administrativt prövningsförfarande eller prövningsförfarande utanför domstol, ska varje registrerad person ha rätt till ett effektivt rättsmedel om den tillsynsmyndighet som är behörig i enlighet med artiklarna 55 och 56 underlåter att behandla ett klagomål eller att informera den registrerade inom tre månader om hur det fortskrider med det klagomål som ingetts med stöd av artikel 77 eller vilket beslut som har fattats med anledning av det.

3. Talan mot en tillsynsmyndighet ska väckas vid domstolarna i den medlemsstat där tillsynsmyndigheten har sitt säte.

4. Om talan väcks mot ett beslut som fattats av en tillsynsmyndighet och som föregicks av ett yttrande från eller beslut av styrelsen inom ramen för mekanismen för enhetlighet ska tillsynsmyndigheten vidarebefordra detta yttrande eller beslut till domstolen.

Artikel 79

Rätt till ett effektivt rättsmedel mot en personuppgiftsansvarig eller ett personuppgiftsbiträde

1. Utan att det påverkar tillgängliga administrativa prövningsförfaranden eller prövningsförfaranden utanför domstol, inbegripet rätten att lämna in ett klagomål till en tillsynsmyndighet i enlighet med artikel 77, ska varje registrerad som anser att hans eller hennes rättigheter enligt denna förordning har åsidosatts som en följd av att hans eller hennes personuppgifter har behandlats på ett sätt som inte är förenligt med denna förordning ha rätt till ett effektivt rättsmedel.

2. Talan mot en personuppgiftsansvarig eller ett personuppgiftsbiträde ska väckas vid domstolarna i den medlemsstat där den personuppgiftsansvarige eller personuppgiftsbiträdet är etablerad. Alternativt får sådan talan väckas vid domstolarna i den medlemsstat där den registrerade har sin hemvist, såvida inte den personuppgiftsansvarige eller personuppgiftsbiträdet är en myndighet i en medlemsstat som agerar inom ramen för sin myndighetsutövning.

([1]) Europaparlamentets och rådets förordning (EG) nr 1049/2001 av den 30 maj 2001 om allmänhetens tillgång till Europaparlamentets, rådets och kommissionens handlingar (EGT L 145, 31.5.2001, s. 43).

Artikel 80

Företrädande av registrerade

1. Den registrerade ska ha rätt att ge ett organ, en organisation eller sammanslutning utan vinstsyfte, som har inrättats på lämpligt sätt i enlighet med lagen i en medlemsstat, vars stadgeenliga mål är av allmänt intresse och som är verksam inom området skydd av registrerades rättigheter och friheter när det gäller skyddet av deras personuppgifter, i uppdrag att lämna in ett klagomål för hans eller hennes räkning, att utöva de rättigheter som avses i artiklarna 77, 78 och 79 för hans eller hennes räkning samt att för hans eller hennes räkning utöva den rätt till ersättning som avses i artikel 82 om så föreskrivs i medlemsstatens nationella rätt.

2. Medlemsstaterna får föreskriva att ett organ, en organisation eller en sammanslutning enligt punkt 1 i den här artikeln, oberoende av en registrerads mandat, har rätt att i den medlemsstaten inge klagomål till den tillsynsmyndighet som är behörig enligt artikel 77 och utöva de rättigheter som avses i artiklarna 78 och 79 om organet, organisationen eller sammanslutningen anser att den registrerades rättigheter enligt den här förordningen har kränkts som en följd av behandlingen.

Artikel 81

Vilandeförklaring av förfaranden

1. Om en behörig domstol i en medlemsstat har information om att förfaranden som rör samma sakfråga vad gäller behandling av samma personuppgiftsansvarige eller personuppgiftsbiträde pågår i en domstol i en annan medlemsstat ska den kontakta denna domstol i den andra medlemsstaten för att bekräfta förekomsten av sådana förfaranden.

2. Om förfaranden som rör samma sakfråga vad gäller behandling av samma personuppgiftsansvarige eller personuppgiftsbiträde pågår i en domstol i en annan medlemstat får alla andra behöriga domstolar än den där förfarandena först inleddes vilandeförklara förfarandena.

3. Om dessa förfaranden prövas i första instans får varje domstol, utom den vid vilken förfarandena först inleddes, också förklara sig obehörig på begäran av en av parterna, om den domstol vid vilken förfarandena först inleddes är behörig att pröva de berörda förfarandena och dess lagstiftning tillåter förening av dessa.

Artikel 82

Ansvar och rätt till ersättning

1. Varje person som har lidit materiell eller immateriell skada till följd av en överträdelse av denna förordning ska ha rätt till ersättning från den personuppgiftsansvarige eller personuppgiftsbiträdet för den uppkomna skadan.

2. Varje personuppgiftsansvarig som medverkat vid behandlingen ska ansvara för skada som orsakats av behandling som strider mot denna förordning. Ett personuppgiftsbiträde ska ansvara för skada uppkommen till följd av behandlingen endast om denne inte har fullgjort de skyldigheter i denna förordning som specifikt riktar sig till personuppgiftsbiträden eller agerat utanför eller i strid med den personuppgiftsansvariges lagenliga anvisningar.

3. Den personuppgiftsansvarige eller personuppgiftsbiträdet ska undgå ansvar enligt punkt 2 om den visar att den inte på något sätt är ansvarig för den händelse som orsakade skadan.

4. Om mer än en personuppgiftsansvarig eller ett personuppgiftsbiträde, eller både en personuppgiftsansvarig och ett personuppgiftsbiträde, har medverkat vid samma behandling, och om de enligt punkterna 2 och 3 är ansvariga för eventuell skada som behandlingen orsakat ska varje personuppgiftsansvarig eller personuppgiftsbiträde hållas ansvarig för hela skadan för att säkerställa att den registrerade får effektiv ersättning.

5. Om en personuppgiftsansvarig eller ett personuppgiftsbiträde, i enlighet med punkt 4, har betalat full ersättning för den skada som orsakats ska den personuppgiftsansvarige eller personuppgiftsbiträdet ha rätt att från de andra personuppgiftsansvariga eller personuppgiftsbiträdena som medverkat vid samma behandling återkräva den del av ersättningen som motsvarar deras del av ansvaret för skadan i enlighet med de villkor som fastställs i punkt 2.

6. Domstolsförfaranden för utövande av rätten till ersättning ska tas upp vid de domstolar som är behöriga enligt den nationella rätten i den medlemsstat som avses i artikel 79.2.

Artikel 83

Allmänna villkor för påförande av administrativa sanktionsavgifter

1. Varje tillsynsmyndighet ska säkerställa att påförande av administrativa sanktionsavgifter i enlighet med denna artikel för sådana överträdelser av denna förordning som avses i punkterna 4, 5 och 6 i varje enskilt fall är effektivt, proportionellt och avskräckande.

2. Administrativa sanktionsavgifter ska, beroende på omständigheterna i det enskilda fallet, påföras utöver eller i stället för de åtgärder som avses i artikel 58.2 a–h och j. Vid beslut om huruvida administrativa sanktionsavgifter ska påföras och om beloppet för de administrativa sanktionsavgifterna i varje enskilt fall ska vederbörlig hänsyn tas till följande:

a) Överträdelsens karaktär, svårighetsgrad och varaktighet med beaktande av den aktuella uppgiftsbehandlingens karaktär, omfattning eller syfte samt antalet berörda registrerade och den skada som de har lidit.

b) Om överträdelsen skett med uppsåt eller genom oaktsamhet.

c) De åtgärder som den personuppgiftsansvarige eller personuppgiftsbiträdet har vidtagit för att lindra den skada som de registrerade har lidit.

d) Graden av ansvar hos den personuppgiftsansvarige eller personuppgiftsbiträdet med beaktande av de tekniska och organisatoriska åtgärder som genomförts av dem i enlighet med artiklarna 25 och 32.

e) Eventuella relevanta tidigare överträdelser som den personuppgiftsansvarige eller personuppgiftsbiträdet gjort sig skyldig till.

f) Graden av samarbete med tillsynsmyndigheten för att komma till rätta med överträdelsen och minska dess potentiella negativa effekter.

g) De kategorier av personuppgifter som påverkas av överträdelsen.

h) Det sätt på vilket överträdelsen kom till tillsynsmyndighetens kännedom, särskilt huruvida och i vilken omfattning den personuppgiftsansvarige eller personuppgiftsbiträdet anmälde överträdelsen.

i) När åtgärder enligt artikel 58.2 tidigare har förordnats mot den berörda personuppgiftsansvarige eller personuppgiftsbiträdet vad gäller samma sakfråga, efterlevnad av dessa åtgärder.

j) Tillämpandet av godkända uppförandekoder i enlighet med artikel 40 eller godkända certifieringsmekanismer i enlighet med artikel 42.

k) Eventuell annan försvårande eller förmildrande faktor som är tillämplig på omständigheterna i fallet, såsom ekonomisk vinst som görs eller förlust som undviks, direkt eller indirekt, genom överträdelsen.

3. Om en personuppgiftsansvarig eller ett personuppgiftsbiträde, med avseende på en och samma eller sammankopplade uppgiftsbehandlingar, uppsåtligen eller av oaktsamhet överträder flera av bestämmelserna i denna förordning får den administrativa sanktionsavgiftens totala belopp inte överstiga det belopp som fastställs för den allvarligaste överträdelsen.

4. Vid överträdelser av följande bestämmelser ska det i enlighet med punkt 2 påföras administrativa sanktionsavgifter på upp till 10 000 000 EUR eller, om det gäller ett företag, på upp till 2 % av den totala globala årsomsättningen under föregående budgetår, beroende på vilket värde som är högst:

a) Personuppgiftsansvarigas och personuppgiftsbiträdens skyldigheter enligt artiklarna 8, 11, 25–39, 42 och 43.

b) Certifieringsorganets skyldigheter enligt artiklarna 42 och 43.

c) Övervakningsorganets skyldigheter enligt artikel 41.4.

5. Vid överträdelser av följande bestämmelser ska det i enlighet med punkt 2 påföras administrativa sanktionsavgifter på upp till 20 000 000 EUR eller, om det gäller ett företag, på upp till 4 % av den totala globala årsomsättningen under föregående budgetår, beroende på vilket värde som är högst:

a) De grundläggande principerna för behandling, inklusive villkoren för samtycke, enligt artiklarna 5, 6, 7 och 9.

b) Registrerades rättigheter enligt artiklarna 12–22.

c) Överföring av personuppgifter till en mottagare i ett tredjeland eller en internationell organisation enligt artiklarna 44–49.

d) Alla skyldigheter som följer av medlemsstaternas lagstiftning som antagits på grundval av kapitel IX.

e) Underlåtenhet att rätta sig efter ett föreläggande eller en tillfällig eller permanent begränsning av behandling av uppgifter eller ett beslut om att avbryta uppgiftsflödena som meddelats av tillsynsmyndigheten i enlighet med artikel 58.2 eller underlåtelse att ge tillgång till uppgifter i strid med artikel 58.1.

6. Vid underlåtenhet att rätta sig efter ett föreläggande från tillsynsmyndigheten i enlighet med artikel 58.2 ska det i enlighet med punkt 2 i den här artikeln påföras administrativa sanktionsavgifter på upp till 20 000 000 EUR eller, om det gäller ett företag, på upp till 4 % av den totala globala årsomsättningen under föregående budgetår, beroende på vilket värde som är högst:

7. Utan att det påverkar tillsynsmyndigheternas korrigerande befogenheter enligt artikel 58.2 får varje medlemsstat fastställa regler för huruvida och i vilken utsträckning administrativa sanktionsavgifter kan påföras offentliga myndigheter och organ som är inrättade i medlemsstaten.

8. Tillsynsmyndighetens utövande av sina befogenheter enligt denna artikel ska omfattas av lämpliga rättssäkerhetsgarantier i enlighet med unionsrätten och medlemsstaternas nationella rätt, inbegripet effektiva rättsmedel och rättssäkerhet.

9. Om det i medlemsstatens rättssystem inte finns några föreskrifter om administrativa sanktionsavgifter får den här artikeln tillämpas så att förfarandet inleds av den behöriga tillsynsmyndigheten och sanktionsavgifterna sedan utdöms av behörig nationell domstol, varvid det säkerställs att rättsmedlen är effektiva och har motsvarande verkan som de administrativa sanktionsavgifter som påförs av tillsynsmyndigheter. De sanktionsavgifter som påförs ska i alla händelser vara effektiva, proportionella och avskräckande. Dessa medlemsstater ska till kommissionen anmäla de bestämmelser i deras lagstiftning som de antar i enlighet med denna punkt senast den 25 maj 2018, samt utan dröjsmål anmäla eventuell senare ändringslagstiftning eller ändringar som berör dem.

Artikel 84

Sanktioner

1. Medlemsstaterna ska fastställa regler om andra sanktioner för överträdelser av denna förordning, särskilt för överträdelser som inte är föremål för administrativa sanktionsavgifter enligt artikel 83, och vidta alla nödvändiga åtgärder för att säkerställa att de genomförs. Dessa sanktioner ska vara effektiva, proportionella och avskräckande.

2. Varje medlemsstat ska till kommissionen anmäla de bestämmelser i sin lagstiftning som den antar i enlighet med punkt 1 senast den 25 maj 2018, samt utan dröjsmål anmäla eventuella senare ändringar som berör dem.

KAPITEL IX

Bestämmelser om särskilda behandlingssituationer

Artikel 85

Behandling och yttrande- och informationsfriheten

1. Medlemsstaterna ska i lag förena rätten till integritet i enlighet med denna förordning med yttrande- och informationsfriheten, inbegripet behandling som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande.

2. Medlemsstaterna ska, för behandling som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande, fastställa undantag eller avvikelser från kapitel II (principer), kapitel III (den registrerades rättigheter), kapitel IV (personuppgiftsansvarig och personuppgiftsbiträde), kapitel V (överföring av personuppgifter till tredjeländer eller internationella organisationer), kapitel VI (oberoende tillsynsmyndigheter), kapitel VII (samarbete och enhetlighet) och kapitel IX (särskilda situationer vid behandling av personuppgifter) om dessa är nödvändiga för att förena rätten till integritet med yttrande- och informationsfriheten.

3. Varje medlemsstat ska till kommissionen anmäla de bestämmelser i sin lagstiftning som den antagit i enlighet med punkt 2, samt utan dröjsmål anmäla eventuell senare ändringslagstiftning eller ändringar som berör dem.

Artikel 86

Behandling och allmänhetens tillgång till allmänna handlingar

Personuppgifter i allmänna handlingar som förvaras av en myndighet eller ett offentligt organ eller ett privat organ för utförande av en uppgift av allmänt intresse får lämnas ut av myndigheten eller organet i enlighet med den unionsrätt eller den medlemsstats nationella rätt som myndigheten eller det offentliga organet omfattas av, för att jämka samman allmänhetens rätt att få tillgång till allmänna handlingar med rätten till skydd av personuppgifter i enlighet med denna förordning.

Artikel 87

Behandling av nationella identifikationsnummer

Medlemsstaterna får närmare bestämma på vilka särskilda villkor ett nationellt identifikationsnummer eller något annat vedertaget sätt för identifiering får behandlas. Ett nationellt identifikationsnummer eller ett annat vedertaget sätt för identifiering ska i sådana fall endast användas med iakttagande av lämpliga skyddsåtgärder för de registrerades rättigheter och friheter enligt denna förordning.

Artikel 88

Behandling i anställningsförhållanden

1. Medlemsstaterna får i lag eller i kollektivavtal fastställa mer specifika regler för att säkerställa skyddet av rättigheter och friheter vid behandling av anställdas personuppgifter i anställningsförhållanden, särskilt när det gäller rekrytering, genomförande av anställningsavtalet inklusive befrielse från i lag eller kollektivavtal stadgade skyldigheter, ledning, planering och organisering av arbetet, jämställdhet och mångfald i arbetslivet, hälsa och säkerhet på arbetsplatsen samt skydd av arbetsgivarens eller kundens egendom men också när det gäller att såväl kollektivt som individuellt utöva och komma i åtnjutande av rättigheter och förmåner som är knutna till anställningen samt att avsluta anställningsförhållandet.

2. Dessa regler ska innehålla lämpliga och specifika åtgärder för att skydda den registrerades mänskliga värdighet, berättigade intressen och grundläggande rättigheter, varvid hänsyn särskilt ska tas till insyn i behandlingen, överföring av personuppgifter inom en koncern eller en grupp av företag som deltar i gemensam ekonomisk verksamhet samt övervakningssystem på arbetsplatsen.

3. Varje medlemsstat ska till kommissionen anmäla de bestämmelser i sin lagstiftning som den antar i enlighet med punkt 1 senast den 25 maj 2018, samt utan dröjsmål anmäla eventuella senare ändringar som berör dem.

Artikel 89

Skyddsåtgärder och undantag för behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål

1. Behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål ska omfattas av lämpliga skyddsåtgärder i enlighet med denna förordning för den registrerades rättigheter och friheter. Skyddsåtgärderna ska säkerställa att tekniska och organisatoriska åtgärder har införts för att se till att särskilt

principen om uppgiftsminimering iakttas. Dessa åtgärder får inbegripa pseudonymisering, under förutsättning att dessa ändamål kan uppfyllas på det sättet. När dessa ändamål kan uppfyllas genom vidare behandling av uppgifter som inte medger eller inte längre medger identifiering av de registrerade ska dessa ändamål uppfyllas på det sättet.

2. Om personuppgifter behandlas för vetenskapliga eller historiska forskningsändamål eller statistiska ändamål får det i unionsrätten eller i medlemsstaternas nationella rätt föreskrivas undantag från de rättigheter som avses i artiklarna 15, 16, 18 och 21 med förbehåll för de villkor och skyddsåtgärder som avses i punkt 1 i den här artikeln i den utsträckning som sådana rättigheter sannolikt kommer att göra det omöjligt eller mycket svårare att uppfylla de särskilda ändamålen, och sådana undantag krävs för att uppnå dessa ändamål.

3. Om personuppgifter behandlas för arkivändamål av allmänt intresse får det i unionsrätten eller i medlemsstaternas nationella rätt föreskrivas om undantag från de rättigheter som avses i artiklarna 15, 16, 18, 19, 20 och 21 med förbehåll för de villkor och skyddsåtgärder som avses i punkt 1 i den här artikeln i den utsträckning som sådana rättigheter sannolikt kommer att göra det omöjligt eller mycket svårare att uppfylla de särskilda ändamålen, och sådana undantag krävs för att uppnå dessa ändamål.

4. Om behandling enligt punkterna 2 och 3 samtidigt har andra ändamål, ska undantagen endast tillämpas på behandling för de ändamål som avses i dessa punkter.

Artikel 90

Tystnadsplikt

1. Medlemsstaterna får anta särskilda bestämmelser för att fastställa tillsynsmyndigheternas befogenheter enligt artikel 58.1 e och f gentemot personuppgiftsansvariga eller personuppgiftsbiträden som enligt unionsrätten eller medlemsstaternas nationella rätt eller bestämmelser som fastställts av behöriga nationella organ omfattas av tystnadsplikt eller andra motsvarande former av förbud mot att lämna ut uppgifter, om det är nödvändigt och står i proportion till vad som behövs för att förena rätten till skydd för personuppgifter och tystnadsplikten. Dessa bestämmelser ska endast tillämpas med avseende på personuppgifter som den personuppgiftsansvarige eller personuppgiftsbiträdet har erhållit i samband med en verksamhet som omfattas av denna tystnadsplikt.

2. Varje medlemsstat ska till kommissionen anmäla de bestämmelser den har antagit i enlighet med punkt 1 senast den 25 maj 2018, samt utan dröjsmål anmäla eventuella ändringar som berör dem.

Artikel 91

Befintliga bestämmelser om dataskydd inom kyrkor och religiösa samfund

1. Om kyrkor och religiösa samfund eller gemenskaper i en medlemsstat vid tidpunkten för ikraftträdandet av denna förordning tillämpar övergripande bestämmelser om skyddet av fysiska personer i samband med behandling, får sådana befintliga bestämmelser fortsätta att tillämpas under förutsättning att de görs förenliga med denna förordning.

2. Kyrkor och religiösa samfund som tillämpar övergripande bestämmelser i enlighet med punkt 1 i denna artikel ska vara föremål för kontroll av en oberoende tillsynsmyndighet som kan vara specifik, förutsatt att den uppfyller de villkor som fastställs i kapitel VI i denna förordning.

KAPITEL X

Delegerade akter och genomförandeakter

Artikel 92

Utövande av delegeringen

1. Befogenheten att anta delegerade akter ges till kommissionen med förbehåll för de villkor som anges i denna artikel.

2. Den befogenhet att anta delegerade akter som avses i artikel 12.8 och artikel 43.8 ska ges till kommissionen tills vidare från och med den 24 maj 2016.

3. Den delegering av befogenhet som avses i artikel 12.8 och artikel 43.8 får när som helst återkallas av Europaparlamentet eller rådet. Ett beslut om återkallelse innebär att delegeringen av den befogenhet som anges i beslutet upphör att gälla. Beslutet får verkan dagen efter det att det offentliggörs i *Europeiska unionens officiella tidning*, eller vid ett senare i beslutet angivet datum. Det påverkar inte giltigheten av delegerade akter som redan har trätt i kraft.

4. Så snart kommissionen antar en delegerad akt ska den samtidigt delge Europaparlamentet och rådet denna.

5. En delegerad akt som antas enligt artikel 12.8 och artikel 43.8 ska träda i kraft endast om varken Europaparlamentet eller rådet har gjort invändningar mot den delegerade akten inom en period av tre månader från den dag då akten delgavs Europaparlamentet och rådet, eller om både Europaparlamentet och rådet, före utgången av den perioden, har underrättat kommissionen om att de inte kommer att invända. Denna period ska förlängas med tre månader på Europaparlamentets eller rådets initiativ.

Artikel 93

Kommittéförfarande

1. Kommissionen ska biträdas av en kommitté. Denna kommitté ska vara en kommitté i den mening som avses i förordning (EU) nr 182/2011.

2. När det hänvisas till denna punkt ska artikel 5 i förordning (EU) nr 182/2011 tillämpas.

3. När det hänvisas till denna punkt ska artikel 8 i förordning (EU) nr 182/2011, jämförd med artikel 5 i samma förordning, tillämpas.

KAPITEL XI

Slutbestämmelser

Artikel 94

Upphävande av direktiv 95/46/EG

1. Direktiv 95/46/EG ska upphöra att gälla med verkan från och med den 25 maj 2018.

2. Hänvisningar till det upphävda direktivet ska anses som hänvisningar till denna förordning. Hänvisningar till arbetsgruppen för skydd av enskilda med avseende på behandlingen av personuppgifter, som inrättades genom artikel 29 i direktiv 95/46/EG, ska anses som hänvisningar till Europeiska dataskyddsstyrelsen, som inrättas genom denna förordning.

Artikel 95

Förhållande till direktiv 2002/58/EG

Denna förordning ska inte innebära några ytterligare förpliktelser för fysiska eller juridiska personer som behandlar personuppgifter inom ramen för tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster i allmänna kommunikationsnät i unionen, när det gäller områden inom vilka de redan omfattas av särskilda skyldigheter för samma ändamål i enlighet med direktiv 2002/58/EG.

Artikel 96

Förhållande till tidigare ingångna avtal

De internationella avtal som rör överföring av personuppgifter till tredjeländer eller internationella organisationer som ingicks av medlemsstaterna före den 24 maj 2016 och som är förenliga med unionsrätten i dess lydelse innan detta datum, ska fortsätta att gälla tills de ändras, ersätts eller återkallas.

Artikel 97

Kommissionsrapporter

1. Senast den 25 maj 2020 och därefter vart fjärde år ska kommissionen överlämna en rapport om tillämpningen och översynen av denna förordning till Europaparlamentet och rådet.

2. Inom ramen för de utvärderingar och översyner som avses i punkt 1 ska kommissionen särskilt undersöka hur följande bestämmelser tillämpas och fungerar:

a) Kapitel V om överföring av personuppgifter till tredjeländer och internationella organisationer, särskilt när det gäller beslut som antagits enligt artikel 45.3 i den här förordningen och beslut som antagits på grundval av artikel 25.6 i direktiv 95/46/EG.

b) Kapitel VII om samarbete och enhetlighet.

3. Med avseende på tillämpningen av punkt 1 får kommissionen begära information från medlemsstaterna och tillsynsmyndigheterna.

4. Kommissionen ska när den utför de utvärderingar och översyner som avses i punkterna 1 och 2 ta hänsyn till ståndpunkter och slutsatser från Europaparlamentet, rådet och andra relevanta organ och källor.

5. Kommissionen ska om nödvändigt överlämna lämpliga förslag om ändring av denna förordning, med särskild hänsyn till informationsteknikens utveckling och mot bakgrund av tendenserna inom informationssamhället.

Artikel 98

Översyn av andra unionsrättsakter om dataskydd

Kommissionen ska, om så är lämpligt, lägga fram lagstiftningsförslag i syfte att ändra andra unionsrättsakter om skydd av personuppgifter, för att säkerställa ett enhetligt och konsekvent skydd för fysiska personer med avseende på behandling. Detta gäller i synnerhet bestämmelserna om skyddet för fysiska personer i samband med behandling som utförs av unionens institutioner, organ och byråer samt om det fria flödet av sådana uppgifter.

Artikel 99

Ikraftträdande och tillämpning

1. Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

2. Den ska tillämpas från och med den 25 maj 2018.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Bryssel den 27 april 2016.

På Europaparlamentets vägnar	*På rådets vägnar*
M. SCHULZ	J.A. HENNIS-PLASSCHAERT
Ordförande	*Ordförande*

Sammanfattning av betänkandet Ny dataskyddslag – Kompletterande bestämmelser till EU:s dataskyddsförordning (SOU 2017:39)

Inledning

EU:s nya dataskyddsförordning ska tillämpas från och med den 25 maj 2018. Dataskyddsförordningen är direkt tillämplig i Sverige men ger utrymme för kompletterande nationella bestämmelser av olika slag.

Vårt övergripande uppdrag har varit att föreslå en ny nationell reglering som på ett generellt plan kompletterar dataskyddsförordningen. I vårt uppdrag har däremot inte ingått att se över de s.k. registerförfattningarna eller annan sektorsspecifik reglering om behandling av personuppgifter. Vi har inte heller haft i uppdrag att analysera eller beskriva vilka förändringar som dataskyddsförordningen i sig innebär. Det är därmed bara ett fåtal av alla de frågor som regleras i dataskyddsförordningen som behandlas eller ens nämns i detta betänkande.

Vi har, inom ramen för vårt uppdrag, strävat efter att den personuppgiftsbehandling som är tillåten i dag i möjligaste mån ska kunna fortsätta. Vårt arbete har alltså inte syftat till att vare sig utvidga eller inskränka möjligheterna till behandling av personuppgifter, annat än då dataskyddsförordningen kräver en sådan förändring.

Ett nytt svenskt regelverk om dataskydd

Vi föreslår att personuppgiftslagen (1998:204) och personuppgiftsförordningen (1998:1191) ska upphävas och att de kompletterande bestämmelser som är av generell karaktär samlas i en ny övergripande lag och förordning om dataskydd. För att betona att författningarna inte är heltäckande, utan endast utgör komplement till dataskyddsförordningen, bör de benämnas lagen med kompletterande bestämmelser till EU:s dataskyddsförordning respektive förordningen med kompletterande bestämmelser till EU:s dataskyddsförordning. Vi har valt att kalla den nya lagen dataskyddslagen i detta betänkande.

Dataskyddsförordningen ska gälla även i verksamhet som inte omfattas av unionsrätten

Behandling av personuppgifter som utförs som ett led i en verksamhet som inte omfattas av unionsrätten, t.ex. i verksamhet som rör nationell säkerhet, omfattas inte av dataskyddsförordningen. Detsamma gäller behandling av personuppgifter i verksamhet som omfattas av EU:s gemensamma utrikes- och säkerhetspolitik. För att säkerställa att det inom varje verksamhet finns ett fullgott skydd av personuppgifter anser vi dock att förordningens bestämmelser i tillämpliga delar bör gälla även i dessa fall. Vårt förslag om utsträckt tillämpningsområde hindrar dock inte att det för en viss sådan verksamhet införs en särskild reglering, om det skulle anses mer lämpligt.

Sektorsspecifika bestämmelser ska ha företräde framför dataskyddslagen

De bestämmelser som vi föreslår är av generell karaktär. På vissa områden kommer det att finnas behov av lag- eller förordningsbestämmelser kring behandling av personuppgifter som avviker från dataskyddslagens reglering. Det kan t.ex. röra sig om bestämmelser som specificerar den rättsliga grunden för en myndighets behandling av personuppgifter, begränsningar av rätten att behandla känsliga personuppgifter i en viss verksamhet eller särskilda förfaranderegler. Vi föreslår att sådana avvikande bestämmelser ska ha företräde framför dataskyddslagen. Det innebär dock inte att de därigenom också får företräde framför dataskyddsförordningen inom det aktuella området. För att en avvikande bestämmelse i exempelvis en registerförfattning ska kunna tillämpas, måste den vara förenlig med dataskyddsförordningen och avse en fråga som får särregleras genom nationell rätt.

Annorlunda förhåller det sig när det gäller verksamhet som inte omfattas av unionsrätten, dvs. där dataskyddsförordningen inte är direkt tillämplig men där den har fått ett utsträckt tillämpningsområde genom dataskyddslagen. I det fallet kan det genom ett undantag i lag eller förordning föreskrivas att dataskyddsförordningen inte ska gälla i verksamheten. Ett sådant undantag kan också ange att endast vissa delar av dataskyddsförordningen inte ska gälla.

Förhållandet till våra grundlagar förändras inte

Våra detaljerade tryck- och yttrandefrihetsgrundlagar är unika i jämförelse med hur motsvarande reglering ser ut i övriga Europa. Dataskyddsförordningen inskränker inte möjligheterna att behandla personuppgifter på det grundlagsreglerade området. Det får inte råda någon osäkerhet kring detta, eftersom det skulle kunna få påverkan på vitala och mycket känsliga delar av den opinionsskapande verksamheten, såsom meddelarfrihet och källskydd. Vi föreslår därför en upplysningsbestämmelse som tydliggör att bestämmelserna i dataskyddsförordningen och i dataskyddslagen inte ska tillämpas i den utsträckning det skulle strida mot grundlagsbestämmelserna om tryck- och yttrandefrihet.

Utanför det grundlagsskyddade området föreslår vi att ett undantag från dataskyddsförordningen införs för sådan behandling av personuppgifter som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande. Vissa av dataskyddsförordningens bestämmelser, bland annat de som rör säkerhet för personuppgifter, ska dock tillämpas även i dessa fall.

Utrymmet för att ge offentlighetsprincipen företräde framför personuppgiftsregleringen är tydligt i dataskyddsförordningen. Tryckfrihetsförordningens reglering om allmänhetens tillgång till handlingar kan alltså fortsätta att tillämpas, även när det gäller allmänna handlingar som innehåller personuppgifter.

Barn som har fyllt 13 år ska i vissa fall kunna samtycka till behandling av personuppgifter

Enligt förordningen ska ett barn ha fyllt 16 år för att självt kunna samtycka till behandling av personuppgifter vid erbjudandet av informationssamhällets tjänster, t.ex. sociala medier, söktjänster och s.k. appar för smarta enheter. Vi föreslår att denna åldersgräns ska sänkas till 13 år i Sverige. För barn yngre än så krävs att samtycket lämnas av vårdnadshavaren eller att barnets samtycke godkänns av denne.

Rättsliga förpliktelser, myndighetsutövning och uppgifter av allmänt intresse ska vara särskilt reglerade för att utgöra rättslig grund

Enligt dataskyddsförordningen måste en rättslig förpliktelse, myndighetsutövning eller uppgift av allmänt intresse vara fastställd i enlighet med nationell rätt eller unionsrätt för att kunna utgöra rättslig grund för behandling av personuppgifter. Vi föreslår bestämmelser i dataskyddslagen som förtydligar hur dessa företeelser fastställs i enlighet med svensk rätt. En rättslig förpliktelse är enligt svensk rätt fastställd om den gäller enligt lag eller annan författning eller följer av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning. Myndighetsutövning fastställs i svensk rätt genom lag eller annan författning. Uppgifter av allmänt intresse är fastställda i enlighet med svensk rätt om de följer av lag eller annan författning eller av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning.

Med anledning av att vårt uppdrag har omfattat arkivfrågor har vi uppmärksammat att enskilda arkivinstitutioner kan sakna en fastställd rättslig grund för behandling av personuppgifter. I avvaktan på den breda översyn av arkivväsendet som regeringen har aviserat, föreslår vi att rättslig grund ska kunna fastställas av Riksarkivet, genom föreskrifter eller beslut i enskilda fall.

Känsliga personuppgifter får behandlas bara om det uttryckligen är tillåtet

Enligt dataskyddsförordningen gäller som huvudregel, liksom tidigare, ett förbud mot behandling av känsliga personuppgifter. Behandling av sådana personuppgifter får ske bara om det finns stöd i någon av förordningens undantagsbestämmelser. Vissa undantag från förbudet följer direkt av förordningen, medan andra förutsätter stöd även i nationell rätt. Vi föreslår att ett sådant stöd ska införas i dataskyddslagen när det gäller nödvändig behandling av personuppgifter på arbetsrättens område, inom hälso- och sjukvård, i social omsorg, i arkivverksamhet och i statistisk verksamhet. Stödet för behandlingen ska vara förenat med vissa restriktioner.

Myndigheter ska få behandla känsliga personuppgifter med stöd av ett nytt myndighetsundantag

Myndigheter har ofta berättigade skäl att behandla känsliga personuppgifter och i många fall sker detta i den registrerades eget intresse. För att säkerställa att nödvändig behandling kan ske även efter det att dataskyddsförordningen börjar gälla bedömer vi att det krävs ett nytt

undantag för behandling av känsliga personuppgifter hos myndigheter. Vi föreslår att sådan behandling ska få ske

– i löpande text om uppgifterna har lämnats i ett ärende eller är nödvändiga för handläggningen av ett ärende,

– om uppgifterna har lämnats till myndigheten och behandlingen krävs enligt lag, eller

– i enstaka fall, om det är absolut nödvändigt för ändamålet med behandlingen och behandlingen inte innebär ett otillbörligt intrång i den registrerades personliga integritet.

Vi föreslår också att det vid behandling som sker med stöd av det nya myndighetsundantaget ska vara förbjudet att använda sökbegrepp som avslöjar känsliga personuppgifter.

Personuppgifter som rör lagöverträdelser ska få behandlas av myndigheter och annars bara om det uttryckligen är tillåtet

Vi föreslår att behandling av personuppgifter som rör fällande domar i brottmål, lagöverträdelser som innefattar brott eller straffprocessuella tvångsmedel även fortsättningsvis ska få utföras av myndigheter.

För att andra än myndigheter ska få behandla sådana uppgifter föreslår vi att det måste finnas uttryckligt stöd i lag eller förordning eller i föreskrifter eller förvaltningsbeslut från Datainspektionen. Vi föreslår ett sådant stöd i lag när det gäller uppgifter som behandlas för arkivändamål av allmänt intresse, förutsatt att behandlingen sker som en följd av de skyldigheter att bevara och vårda handlingar som anges i arkivlagstiftningen och andra föreskrifter.

Personnummer får under vissa förutsättningar behandlas även i fortsättningen

Vi föreslår att uppgifter om personnummer eller samordningsnummer även fortsättningsvis ska få behandlas när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl.

Det finns begränsningar för när arkiverade uppgifter och statistikuppgifter får användas för åtgärder mot den registrerade

Personuppgifter som behandlas enbart för arkivändamål av allmänt intresse eller för statistiska ändamål får enligt vårt förslag inte användas för att vidta åtgärder i fråga om den registrerade, annat än om det finns synnerliga skäl med hänsyn till den registrerades vitala intressen.

Begränsningen i fråga om arkiverade uppgifter ska inte gälla för myndigheter. Det ska däremot begränsningen rörande statistikuppgifter göra.

Rätten till registerutdrag och information m.m. ska i vissa fall vara begränsad

Den registrerades rättigheter stärks genom dataskyddsförordningen. Dessa rättigheter är dock inte ovillkorliga. Vissa viktiga undantag från rättigheterna regleras direkt i förordningen. Vi föreslår därutöver att rätten till information och s.k. registerutdrag inte ska gälla uppgifter som

omfattas av sekretess. Rätten till registerutdrag ska som huvudregel inte heller gälla personuppgifter som finns i löpande text som utgör utkast eller minnesanteckning. Hos Riksarkivet och andra arkivmyndigheter ska rätten till registerutdrag, rättelse m.m. vara begränsad när det gäller personuppgifter som finns i arkivmaterial som tagits emot för förvaring av myndigheten.

Vissa beslut som fattas av en personuppgiftsansvarig myndighet får överklagas till domstol

I likhet med vad som gäller enligt personuppgiftslagen ska vissa beslut som en myndighet fattar i egenskap av personuppgiftsansvarig kunna överklagas till allmän förvaltningsdomstol. Det gäller sådana beslut som myndigheten fattar med anledning av att den registrerade utövar sina rättigheter enligt dataskyddsförordningen. Det kan t.ex. röra sig om avslagsbeslut på begäran om att den registrerade ska få tillgång till sina personuppgifter, att uppgifter ska rättas eller raderas eller att en behandling ska begränsas.

Den registrerade kan begära skadestånd

Den registrerade har enligt dataskyddsförordningen rätt till ersättning från den personuppgiftsansvarige eller ett personuppgiftsbiträde om skada har uppstått på grund av överträdelser av förordningen. Vi föreslår att det i dataskyddslagen förtydligas att denna rätt till skadestånd även gäller vid överträdelser av bestämmelser i dataskyddslagen och andra författningar som kompletterar förordningen.

Datainspektionen ska utöva tillsyn

Datainspektionen ska vara den myndighet som ska utöva tillsyn och övervaka att bestämmelserna i dataskyddsförordningen och dataskyddslagen efterlevs. Inspektionens tillsynsbefogenheter anges i dataskyddsförordningen. Dessa befogenheter ska enligt vårt förslag gälla även vid tillsynen över att dataskyddslagen och annan kompletterande lagstiftning följs.

Datainspektionens beslut enligt dataskyddsförordningen och dataskyddslagen får överklagas till allmän förvaltningsdomstol.

Datainspektionen ska behandla klagomål inom tre månader

Om en registrerad anser att personuppgifter behandlas på ett sätt som strider mot dataskyddsförordningen kan ett klagomål lämnas in till Datainspektionen. Klagomålet ska behandlas inom tre månader. Om det inte sker får den registrerade enligt vårt förslag begära ett besked i frågan om Datainspektionen avser att utöva tillsyn eller inte. Om Datainspektionen behöver mer tid för att behandla klagomålet, får begäran avslås genom ett motiverat beslut. Den registrerade får överklaga detta beslut till allmän förvaltningsdomstol genom en s.k. dröjsmålstalan.

Sanktionsavgift kan tas ut även av myndigheter som gör fel

Genom dataskyddsförordningen införs en möjlighet för Datainspektionen att ta ut en administrativ sanktionsavgift av ett företag eller andra enskilda som bryter mot dataskyddsregleringen. En sådan sanktionsavgift ska enligt vårt förslag även kunna tas ut av en myndighet.

Vi föreslår inte någon straffbestämmelse motsvarande den som gäller enligt personuppgiftslagen.

Sekretessfrågor

Genom dataskyddsförordningen införs en skyldighet för myndigheter och vissa företag att utse ett dataskyddsombud. Ombudet ska vara bundet av sekretess enligt unionsrätten eller den nationella rätten.

För dataskyddsombud som deltar i det allmännas verksamhet gäller offentlighets- och sekretesslagens bestämmelser om sekretess. För den privata sektorn föreslår vi att tystnadsplikt ska gälla för dataskyddsombud i fråga om sådant som ombudet har fått veta om enskilds personliga eller ekonomiska förhållanden.

Konsekvenser

Dataskyddsförordningens direkt tillämpliga bestämmelser kommer att leda till konsekvenser, både för det allmänna och för enskilda. Vi har dock inte haft i uppgift att bedöma eller redovisa dessa konsekvenser. I vårt uppdrag ingår däremot att bedöma konsekvenserna av våra förslag, i den mån dessa medför förändringar jämfört med vad som gäller i dag.

Våra förslag innebär att Riksarkivet, Datainspektionen och de allmänna förvaltningsdomstolarna får något fler arbetsuppgifter. Vi bedömer dock att kostnadsökningarna för berörda aktörer inte kommer att bli större än att de ryms inom de befintliga anslagen.

Våra förslag medför inga nya kostnader eller ökad administrativ börda för enskilda.

Vi anser att förslagen stärker skyddet för enskildas personliga integritet.

Förslag till lag med kompletterande bestämmelser till EU:s dataskyddsförordning

Härigenom föreskrivs följande.

1 kap. Inledande bestämmelser

1 § Denna lag kompletterar Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), nedan kallad dataskyddsförordningen.

Termer och uttryck som används i denna lag har samma betydelse som i dataskyddsförordningen.

2 § Bestämmelserna i dataskyddsförordningen, i den ursprungliga lydelsen, och i denna lag ska i tillämpliga delar gälla även vid behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av unionsrätten och i verksamhet som omfattas av avdelning V kapitel 2 i fördraget om Europeiska unionen.

Avvikande bestämmelser i annan författning

3 § Om en annan lag eller en förordning innehåller någon bestämmelse som rör behandling av personuppgifter och som avviker från denna lag tillämpas den bestämmelsen.

Förhållandet till tryck- och yttrandefriheten

4 § Bestämmelserna i dataskyddsförordningen och i denna lag ska inte tillämpas i den utsträckning det skulle strida mot bestämmelserna om tryck- och yttrandefrihet i tryckfrihetsförordningen eller yttrandefrihetsgrundlagen.

Bestämmelserna i kapitel II och III, artiklarna 24–30 och 35–43 och kapitel V i dataskyddsförordningen samt i 2–5 kap. denna lag ska inte tillämpas på behandling av personuppgifter som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande.

Organ som ska jämställas med myndigheter

5 § Vid tillämpningen av 3 kap. 3 § 2 och 4 § samt 4 kap. 1 § andra stycket ska andra organ än myndigheter jämställas med myndigheter, i den utsträckning bestämmelserna om allmänna handlingar och sekretess i tryckfrihetsförordningen och offentlighets- och sekretesslagen (2009:400) gäller i organets verksamhet.

Tystnadsplikt för dataskyddsombud

6 § Den som utsetts till dataskyddsombud enligt artikel 37 i dataskyddsförordningen får inte obehörigen röja det som han eller hon vid fullgörandet av sin uppgift har fått veta om enskilds personliga och ekonomiska förhållanden.

I det allmännas verksamhet tillämpas offentlighets- och sekretesslagen (2009:400) i stället för första stycket.

2 kap. Rättslig grund

1 § Av dataskyddsförordningen framgår att personuppgifter får behandlas endast om minst ett av de villkor som anges i artikel 6.1 i förordningen är uppfyllt.

2 § Vid erbjudande av informationssamhällets tjänster direkt till ett barn, ska vid tillämpningen av artikel 6.1 a i dataskyddsförordningen behandling av personuppgifter som rör ett barn vara tillåten om barnet är minst 13 år. Om barnet är under 13 år ska sådan behandling vara tillåten endast om och i den mån samtycke ges eller godkänns av den person som har föräldraansvar för barnet.

Rättslig förpliktelse

3 § Personuppgifter får behandlas med stöd av artikel 6.1 c i dataskyddsförordningen om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna fullgöra en rättslig förpliktelse som

1. gäller enligt lag eller annan författning,
2. följer av kollektivavtal, eller
3. följer av beslut som har meddelats med stöd av lag eller annan författning.

Uppgift av allmänt intresse och myndighetsutövning

4 § Personuppgifter får behandlas med stöd av artikel 6.1 e i dataskyddsförordningen om behandlingen är nödvändig

1. för att den personuppgiftsansvarige ska kunna utföra en uppgift av allmänt intresse som följer av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning, eller
2. som ett led i den personuppgiftsansvariges myndighetsutövning enligt lag eller annan författning.

Enskilda arkiv

5 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om behandling av personuppgifter för arkivändamål av allmänt intresse, när det gäller andra enskilda organ än de som omfattas av bestämmelserna om allmänna handlingar och sekretess i tryckfrihetsförordningen och offentlighets- och sekretesslagen (2009:400).

Den myndighet som regeringen bestämmer får även i enskilda fall besluta att sådana enskilda organ som avses i första stycket får behandla personuppgifter för arkivändamål av allmänt intresse.

3 kap. Vissa kategorier av personuppgifter

Känsliga personuppgifter

1 § Utöver vad som framgår av artikel 9.2 a, c, d, e eller f i dataskyddsförordningen får sådana särskilda kategorier av personuppgifter som anges i artikel 9.1 i dataskyddsförordningen (känsliga personuppgifter) behandlas om förutsättningarna i någon av 2–8 §§ är uppfyllda.

Arbetsrätt

2 § Känsliga personuppgifter får med stöd av artikel 9.2 b i dataskyddsförordningen behandlas om det är nödvändigt för att den personuppgiftsansvarige eller den registrerade ska kunna fullgöra sina skyldigheter och utöva sina särskilda rättigheter inom arbetsrätten.

Personuppgifter som behandlas med stöd av första stycket får lämnas ut till tredje part endast om det inom arbetsrätten finns en skyldighet att göra det eller om den registrerade uttryckligen har samtyckt till utlämnandet.

Myndigheters behandling i vissa fall

3 § Känsliga personuppgifter får med stöd av artikel 9.2 g i dataskyddsförordningen behandlas av en myndighet

1. i löpande text om uppgifterna har lämnats i ett ärende eller är nödvändiga för handläggningen av ett ärende,
2. om uppgifterna har lämnats till myndigheten och behandlingen krävs enligt lag, eller
3. i enstaka fall, om det är absolut nödvändigt för ändamålet med behandlingen och behandlingen inte innebär ett otillbörligt intrång i den registrerades personliga integritet.

4 § Vid behandling som sker enbart med stöd av 3 § får en myndighet inte använda sökbegrepp som avslöjar känsliga person-uppgifter.

Hälso- och sjukvård och social omsorg

5 § Känsliga personuppgifter får med stöd av artikel 9.2 h i dataskyddsförordningen behandlas om behandlingen är nödvändig av skäl som hör samman med

1. förebyggande hälso- och sjukvård och yrkesmedicin,
2. bedömningen av en arbetstagares arbetskapacitet,
3. medicinska diagnoser,
4. tillhandahållande av hälso- och sjukvård eller behandling,
5. social omsorg, eller
6. förvaltning av social omsorg, hälso- och sjukvårdstjänster samt deras system.

Behandling enligt första stycket får ske under förutsättning att kravet på tystnadsplikt i artikel 9.3 i dataskyddsförordningen är uppfyllt.

Arkiv

6 § Känsliga personuppgifter får med stöd av artikel 9.2 j i dataskyddsförordningen behandlas för arkivändamål av allmänt intresse om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna följa föreskrifter om bevarande och vård av arkiv.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om att känsliga personuppgifter får behandlas för arkivändamål av allmänt intresse även i andra fall än de som avses i första stycket.

Den myndighet som regeringen bestämmer får även i enskilda fall besluta att andra enskilda organ än de som omfattas av bestämmelserna om allmänna handlingar och sekretess i tryckfrihetsförordningen och offentlighets- och sekretesslagen (2009:400) får behandla känsliga personuppgifter för arkivändamål av allmänt intresse.

Statistik

7 § Känsliga personuppgifter får med stöd av artikel 9.2 j i dataskyddsförordningen behandlas om behandlingen är nödvändig för statistiska ändamål och samhällsintresset av det statistikprojekt där behandlingen ingår klart väger över den risk för otillbörligt intrång i enskildas personliga integritet som behandlingen kan innebära.

Bemyndigande

8 § Regeringen får meddela föreskrifter om ytterligare undantag från förbudet att behandla känsliga personuppgifter i artikel 9.1 i dataskyddsförordningen om det behövs med hänsyn till ett viktigt allmänt intresse.

Personuppgifter som rör lagöverträdelser

Behandling under kontroll av myndighet

9 § Personuppgifter som rör fällande domar i brottmål, lagöverträdelser som innefattar brott eller straffprocessuella tvångsmedel får enligt artikel 10 i dataskyddsförordningen behandlas av myndigheter.

10 § Den myndighet som regeringen bestämmer får i enskilda fall besluta att andra än myndigheter får behandla sådana uppgifter som avses i 9 §.

Arkiv

11 § Behandling av sådana personuppgifter som avses i 9 § får ske om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna följa föreskrifter om bevarande och vård av arkiv.

Bemyndigande

12 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om i vilka fall andra än myndigheter får behandla sådana personuppgifter som avses i 9 §.

Personnummer och samordningsnummer

13 § Uppgifter om personnummer eller samordningsnummer får behandlas utan samtycke endast när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl.

14 § Regeringen får meddela ytterligare föreskrifter om i vilka fall behandling av personnummer och samordningsnummer är tillåten.

4 kap. Användningsbegränsningar

Arkiverade personuppgifter

1 § Personuppgifter som behandlas enbart för arkivändamål av allmänt intresse får inte användas för att vidta åtgärder i fråga om den registrerade, annat än om det finns synnerliga skäl med hänsyn till den registrerades vitala intressen.

Begränsningen i första stycket hindrar dock inte myndigheter från att använda personuppgifter som finns i allmänna handlingar.

Statistikuppgifter

2 § Personuppgifter som behandlas enbart för statistiska ändamål får inte användas för att vidta åtgärder i fråga om den registrerade, annat än om det finns synnerliga skäl med hänsyn till den registrerades vitala intressen.

5 kap. Begränsningar av vissa rättigheter och skyldigheter

Information och tillgång till personuppgifter

1 § Den registrerades rätt till information och tillgång till personuppgifter enligt artiklarna 13–15 i dataskyddsförordningen gäller inte sådana uppgifter som den personuppgiftsansvarige inte får lämna ut till den registrerade enligt lag eller annan författning eller enligt beslut som har meddelats med stöd av författning.

Om den personuppgiftsansvarige inte är en myndighet gäller undantaget i första stycket även för uppgifter som hos en myndighet skulle ha varit sekretessbelagda enligt offentlighets- och sekretesslagen (2009:400).

2 § Bestämmelsen om den registrerades rätt till tillgång till personuppgifter i artikel 15 i dataskyddsförordningen gäller inte personuppgifter i löpande text som inte fått sin slutliga utformning när begäran gjordes eller som utgör minnesanteckning eller liknande.

Undantaget i första stycket gäller inte om personuppgifterna

1. har lämnats ut till tredje part,
2. behandlas enbart för arkivändamål av allmänt intresse eller statistiska ändamål eller,
3. har behandlats under längre tid än ett år i löpande text som inte fått sin slutliga utformning.

Bemyndigande

3 § Regeringen får meddela föreskrifter om ytterligare begränsningar av vissa rättigheter och skyldigheter enligt artikel 23 i dataskyddsförordningen.

6 kap. Tillsynsmyndighetens handläggning och beslut

Befogenheter

1 § De befogenheter som tillsynsmyndigheten har enligt artikel 58.1, 58.2 och 58.3 i dataskyddsförordningen gäller även vid tillsyn över efterlevnaden av bestämmelserna i denna lag och andra författningar som kompletterar dataskyddsförordningen.

Ansökan hos allmän förvaltningsdomstol

2 § Om tillsynsmyndigheten vid handläggningen av ett ärende finner att det finns skäl att ifrågasätta giltigheten av en unionsrättsakt som påverkar tillämpningen av dataskyddsförordningen i ärendet, får tillsynsmyndigheten hos allmän förvaltningsdomstol ansöka om att en åtgärd enligt artikel 58.2 i dataskyddsförordningen ska vidtas.

Ansökan ska göras hos den förvaltningsrätt som är behörig att pröva ett överklagande av tillsynsmyndighetens beslut.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Kommunikation

3 § Innan tillsynsmyndigheten fattar ett beslut som avses i artikel 58.2 i dataskyddsförordningen, ska den som beslutet gäller ges tillfälle att inom en bestämd tid yttra sig över allt material av betydelse för beslutet, om det inte är uppenbart obehövligt.

Om saken är brådskande får myndigheten, i avvaktan på yttrandet, besluta att behandlingen av personuppgifter tillfälligt ska begränsas eller förbjudas i enlighet med artikel 58.2 f i dataskyddsförordningen. Det tillfälliga beslutet ska omprövas, när tiden för yttrande har gått ut.

Delgivning

4 § Ett beslut som avses i 3 § första stycket ska delges, om det inte är uppenbart obehövligt. Delgivning enligt 34–37 §§ delgivningslagen (2010:1932) får användas endast om det finns särskild anledning att anta att mottagaren har avvikit eller på annat sätt håller sig undan.

Besked angående handläggningen av ett klagomål

5 § Om tillsynsmyndigheten inte inom tre månader från den dag då ett klagomål kom in till myndigheten har behandlat klagomålet, ska tillsynsmyndigheten på skriftlig begäran av den registrerade antingen lämna besked i frågan om myndigheten avser att utöva tillsyn med anledning av klagomålet, eller i ett särskilt beslut avslå begäran om besked.

Besked eller beslut enligt första stycket ska meddelas inom två veckor från den dag då begäran om besked kom in till myndigheten.

Om tillsynsmyndigheten har avslagit en begäran om besked enligt första stycket, har den registrerade inte rätt till ett nytt besked i ärendet förrän tidigast tre månader efter det att myndighetens beslut meddelades.

7 kap. Administrativa sanktionsavgifter

1 § Sanktionsavgift får tas ut av en myndighet vid överträdelser som avses i artikel 83.4, 83.5 och 83.6 i dataskyddsförordningen, varvid artikel 83.1, 83.2 och 83.3 i förordningen ska tillämpas.

Vid överträdelser som avses i artikel 83.4 i dataskyddsförordningen ska avgiften bestämmas till högst 10 000 000 kronor och annars till högst 20 000 000 kronor.

2 § Sanktionsavgift får tas ut vid överträdelser av artikel 10 i dataskyddsförordningen, varvid artikel 83.1, 83.2 och 83.3 i förordningen ska tillämpas. Avgiftens storlek ska bestämmas med tillämpning av artikel 83.5 i förordningen.

3 § Sanktionsavgift får inte beslutas, om den som avgiften ska tas ut av inte har fått tillfälle att yttra sig enligt 6 kap. 3 § inom fem år från den dag då överträdelsen ägde rum.

4 § En sanktionsavgift som beslutats enligt dataskyddsförordningen eller denna lag tillfaller staten.

8 kap. Skadestånd och rättsmedel

Skadestånd

1 § Rätten till ersättning enligt artikel 82 i dataskyddsförordningen gäller även vid överträdelser av bestämmelser i denna lag och andra författningar som kompletterar dataskyddsförordningen.

Överklagande av beslut som fattats av en myndighet i egenskap av personuppgiftsansvarig

2 § Beslut enligt artiklarna 12.5, 15–19 eller 21 i dataskyddsförordningen som har meddelats av en myndighet i egenskap av personuppgiftsansvarig får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

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

Dröjsmålstalan

3 § Tillsynsmyndighetens beslut att avslå en begäran om besked enligt 6 kap. 5 § får överklagas till allmän förvaltningsdomstol.

Om domstolen bifaller överklagandet, ska den förelägga tillsynsmyndigheten att inom en bestämd tid lämna besked till den registrerade i frågan om tillsyn kommer att utövas.

Domstolens beslut får inte överklagas.

Överklagande av tillsynsmyndighetens beslut

4 § Tillsynsmyndighetens beslut enligt dataskyddsförordningen och enligt 7 kap. 1 och 2 §§ denna lag får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Överklagande av beslut i enskilda fall

5 § Beslut enligt 2 kap. 5 § andra stycket, 3 kap. 6 § tredje stycket och 3 kap. 10 § denna lag får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Överklagandeförbud

6 § Andra beslut enligt denna lag än de som avses i 2–5 §§ och 6 kap. 2 § får inte överklagas.

---

1. Denna lag träder i kraft den 25 maj 2018.
2. Genom lagen upphävs personuppgiftslagen (1998:204).
3. Den upphävda lagen gäller dock fortfarande i den utsträckning som det i en annan lag eller förordning finns bestämmelser som innehåller hänvisningar till den lagen.
4. Äldre föreskrifter gäller fortfarande för ärenden hos Datainspektionen som har inletts men inte avgjorts före ikraftträdandet.
5. Äldre föreskrifter gäller fortfarande för överklagande av beslut som har meddelats med stöd av dessa föreskrifter.
6. Äldre föreskrifter om skadestånd gäller fortfarande för skada som har orsakats före ikraftträdandet.
7. Äldre föreskrifter gäller fortfarande för överträdelser som har skett före ikraftträdandet.

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

Härigenom föreskrivs att 10 kap. 27 §, 21 kap. 7 § och 40 kap. 5 § samt rubriken närmast före 21 kap. 7 § offentlighets- och sekretesslagen (2009:400) ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
10 kap.	
27 §[2]	
Utöver vad som följer av 2, 3, 5 och 15–26 §§ 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.	
Första stycket gäller inte i fråga om sekretess enligt 24 kap. 2 a och 8 §§, 25 kap. 1–8 §§, 26 kap. 1–6 §§, 29 kap. 1 och 2 §§, 31 kap. 1 § första stycket, 2 och 12 §§, 33 kap. 2 §, 36 kap. 3 § samt 40 kap. 2 och 5 §§.	
Första stycket gäller inte heller om utlämnandet strider mot lag eller förordning *eller föreskrift som har meddelats med stöd av personuppgiftslagen (1998:204)*.	Första stycket gäller inte heller om utlämnandet strider mot lag eller förordning.
21 kap.	
Behandling i strid med *personuppgiftslagen*	Behandling i strid med *dataskyddsregleringen*
7 §	
Sekretess gäller för personuppgift, om det kan antas att ett utlämnande *skulle medföra att uppgiften* behandlas i strid med *personuppgiftslagen (1998:204)*.	Sekretess gäller för personuppgift, om det kan antas att *uppgiften efter* ett utlämnande kommer att behandlas i strid med *Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), i den ursprungliga lydelsen, eller lagen (2018:00) med kompletterande bestämmelser till EU:s dataskyddsförordning*.

[2] Senaste lydelse 2013:795.

40 kap.

5 §

Sekretess gäller i verksamhet för enbart teknisk bearbetning eller teknisk lagring för någon annans räkning av personuppgifter som avses i *personuppgiftslagen (1998:204) för uppgift om en enskilds personliga eller ekonomiska förhållanden*.	Sekretess gäller *för uppgift om en enskilds personliga eller ekonomiska förhållanden* i verksamhet för enbart teknisk bearbetning eller teknisk lagring för någon annans räkning av *sådana* personuppgifter som avses i *artikel 4.1 i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)*.

Denna lag träder i kraft den 25 maj 2018.

Förteckning över remissinstanserna (SOU 2017:39)

Remissvar har lämnats av Riksdagens ombudsmän, Riksrevisionen, Svea hovrätt, Hovrätten för Västra Sverige, Södertörns tingsrätt, Umeå tingsrätt, Kammarrätten i Stockholm, Kammarrätten i Göteborg, Kammarrätten i Jönköping, Förvaltningsrätten i Stockholm, Förvaltningsrätten i Malmö, Förvaltningsrätten i Jönköping, Förvaltningsrätten i Linköping, Justitiekanslern, Hyres- och arrendenämnden i Stockholm, Domstolsverket, Åklagarmyndigheten, Polismyndigheten, Säkerhetspolisen, Brottsoffermyndigheten, Säkerhets- och integritetsskyddsnämnden, Kriminalvården, Brottsförebyggande rådet, Rättsmedicinalverket, Statens haverikommission, Myndigheten för samhällsskydd och beredskap, Kustbevakningen, Migrationsverket, Datainspektionen, Styrelsen för ackreditering och teknisk kontroll, Kommerskollegium, Försvarsmakten, Försvarets radioanstalt, Totalförsvarets forskningsinstitut, Totalförsvarets rekryteringsmyndighet, Försäkringskassan, Socialstyrelsen, Inspektionen för vård och omsorg, Läkemedelsverket, Hälso- och sjukvårdens ansvarsnämnd, Folkhälsomyndigheten, Myndigheten för vård- och omsorgsanalys, Statens institutionsstyrelse, Barnombudsmannen, Forskningsrådet för hälsa, arbetsliv och välfärd, Tandvårds- och läkemedelsförmånsverket, Inspektionen för socialförsäkringen, Pensionsmyndigheten, E-hälsomyndigheten, Tullverket, Finansinspektionen, Skatteverket, Kronofogdemyndigheten, Kammarkollegiet, Statistiska centralbyrån, Arbetsgivarverket, Tillväxtverket, Havs- och vattenmyndigheten, Försvarets materielverk, Livsmedelsverket, E-legitimationsnämnden, Specialpedagogiska skolmyndigheten, Överklagandenämnden för studiestöd, Verket för innovationssystem, Länsstyrelsen i Stockholms län, Länsstyrelsen i Östergötlands län, Länsstyrelsen i Kronobergs län, Länsstyrelsen i Gotlands län, Länsstyrelsen i Skåne län, Länsstyrelsen i Västra Götalands län, Länsstyrelsen i Värmlands län, Länsstyrelsen i Gävleborgs län, Länsstyrelsen i Västernorrlands län, Länsstyrelsen i Norrbottens län, Statskontoret, Statens servicecenter, Konsumentverket, Statens skolverk, Statens skolinspektion, Myndigheten för ungdoms- och civilsamhällesfrågor, Myndigheten för yrkeshögskolan, Universitetskanslersämbetet, Universitets- och högskolerådet, Kungliga Biblioteket, Vetenskapsrådet, Centrala etikprövningsnämnden, Centrala studiestödsnämnden, Uppsala universitet, Örebro universitet, Lunds universitet, Göteborgs universitet, Umeå universitet, Kungliga tekniska högskolan, Karolinska institutet, Post- och telestyrelsen, Transportstyrelsen, Konkurrensverket, Patent- och registreringsverket, Bolagsverket, Regelrådet, Statens jordbruksverk, Lantmäteriet, Riksarkivet, Statens medieråd, Myndigheten för press, radio och TV, Valmyndigheten, Diskrimineringsombudsmannen, Arbetsförmedlingen, Arbetsmiljöverket, Institutet för arbetsmarknads- och utbildningspolitisk utvärdering, Inspektionen för arbetslöshetsförsäkringen, Dorotea kommun, Falköpings kommun, Grästorps kommun, Karlskrona kommun, Kristinehamns kommun, Malmö kommun, Mullsjö kommun, Munkedals kommun, Mörbylånga kommun, Piteå kommun, Skurups kommun, Stockholms kommun, Töreboda kommun, Västra

Götalands läns landsting, Västerbottens läns landsting, Barnens rätt i samhället, Centrum för näringslivshistoria, Forum för dataskydd, IT& Telekomföretagen, Landsorganisationen i Sverige, Svensk Handel, Almega, Teknikföretagen, Vårdföretagarna, Läkemedelsindustriföreningen, Sveriges konsumenter, Riksidrottsförbundet, Småföretagarnas riksförbund, Stiftelsen för internetinfrastruktur, Surfa lugnt, Svensk Försäkring, Svenska bankföreningen, Svenska journalistförbundet, Svenskt Näringsliv, Sveriges advokatsamfund, Sveriges allmännyttiga bostadsföretag, Sveriges Akademikers Centralorganisation, Sveriges Kommuner och Landsting, Sveriges Radio AB, Sveriges Television AB, Swedish Direct Marketing Association, Tidningsutgivarna, Tjänstemännens centralorganisation, Svenskt Friluftsliv, Dataspelsbranschen, Svensk inkasso och Institutet för språk och folkminnen.

Askersunds kommun, Borgholms kommun, Bräcke kommun, Danderyds kommun, Ekerö kommun, Eksjö kommun, Falu kommun, Kramfors kommun, Lycksele kommun, Nordmalings kommun, Storfors kommun, Strömstads kommun, Timrå kommun, Vansbro kommun, Västerås kommun, Örkelljunga kommun, Skåne läns landsting, Arkivrådet AAS, Civil Rights Defenders, Dataföreningen i Sverige, FAI, Handikappförbunden, Postnord AB, Svenska avdelningen av Internationella juristkommissionen, Svenska sektionen av Amnesty International, Sveriges apoteksförening, Sveriges universitets- och högskoleförbund, Svensk Adressändring AB och Swedish Incubators & Science Parks har avstått från att lämna synpunkter på förslagen i betänkandet eller har inte svarat på remissen.

Synpunkter har även lämnats av Säkerhets- och försvarsföretagen, Dataskydd.net, Sveriges Elevkårer, Svenska Brukshundsklubben, Friluftsfrämjandet, Föreningen Sveriges länsarkivarier, Villaägarnas Riksförbund, Srf Konsulternas förbund, Lärarnas riksförbund, Svenska Jägareförbundet, Collectum, Stiftelsen Svenska Filminstitutet, Sveriges sportfiske- och fiskevårdsförbund, Sveriges Ingenjörer, Sveriges läkareförbund, Näringslivets regelnämnd, Svenska kyrkan, Svenska kanotförbundet, Arbetarrörelsens arkiv och bibliotek samt Finansbolagen.

Sammanfattning av promemorian Kompletterande promemoria till betänkandet Ny dataskyddslag (SOU 2017:39)

Promemorians bakgrund och syfte

Behandling av personuppgifter är i många fall en gränsöverskridande aktivitet. Det är till exempel inte ovanligt att den som behandlar personuppgifter om personer i Sverige inte själv är etablerad genom ett verksamhetsställe i landet. På motsvarande sätt kan svenska företag och organisationer behandla personuppgifter om individer i andra länder utan att ha något verksamhetsställe där. I dessa situationer uppkommer fråga om vilket lands lag som ska tillämpas – den lag som gäller i den registrerades land (effektlandsprincipen) eller den lag som gäller i det land där den personuppgiftsansvarige är etablerad (etableringslandsprincipen). Dataskyddsförordningen innehåller inte några regler om vilken nationell rätt som ska gälla vid gränsöverskridande personuppgiftsbehandling. Dataskyddsutredningen har inte heller behandlat frågan om dataskyddslagens territoriella tillämpningsområde i det remitterade betänkandet.

Det finns ett behov av att reglera dataskyddslagens territoriella tillämpningsområde

Dataskyddsförordningen innehåller, till skillnad från dataskyddsdirektivet, inte någon reglering om tillämplig nationell lag. Förordningens territoriella tillämpningsområde anges dock i artikel 3. Eftersom förordningen inte reglerar tillämpningsområdet för kompletterande nationell lagstiftning bör medlemsstaterna i princip vara fria att bestämma detta själva. Det är ur ett tillämpningsperspektiv viktigt att det står klart i vilka fall dataskyddslagen gäller vid gränsöverskridande behandling av personuppgifter. Av rättssäkerhetsskäl bör det därför införas en uttrycklig bestämmelse om det territoriella tillämpningsområdet i dataskyddslagen.

En huvudregel som följer förordningens principer

Etableringslandsprincipen kan sägas vara utgångspunkten i dataskyddsförordningens reglering om det territoriella tillämpningsområdet. Ett val av etableringslandsprincipen som huvudregel för dataskyddslagens tillämpningsområde skulle således harmoniera väl med regleringen i förordningen. Det kan också konstateras att personuppgiftslagens reglering om tillämpningsområdet utgår från etableringslandsprincipen. Ett val av denna princip skulle således innebära en kontinuitet i förhållande till den nuvarande regleringen.

Mot denna bakgrund bör etableringslandsprincipen gälla som utgångspunkt för dataskyddslagens territoriella tillämpningsområde, i fråga om behandling som utförs inom ramen för den verksamhet som bedrivs vid ett verksamhetsställe i Sverige. Det saknar därmed betydelse var behandlingen faktiskt utförs och var den registrerade befinner sig. Omvänt kommer lagen, enligt huvudregeln, inte att gälla för personuppgiftsansvariga som saknar verksamhetsställe i Sverige, även om de behandlar uppgifter om personer i Sverige. Lagen kommer inte heller att gälla för

behandling som utförs endast inom ramen för verksamhet som den personuppgiftsansvarige bedriver vid ett verksamhetsställe i ett annat EU-land, även om den personuppgiftsansvarige också har ett verksamhetsställe i Sverige.

Dataskyddsförordningen är också tillämplig på behandling av personuppgifter som utförs av en personuppgiftsansvarig som inte är etablerad i unionen, men på en plats där en medlemsstats nationella rätt gäller enligt folkrätten. På motsvarande sätt bör dataskyddslagen vara tillämplig vid behandling av personuppgifter som utförs av personuppgiftsansvariga som inte är etablerade i Sverige, men på en plats där svensk rätt gäller enligt folkrätten, till exempel vid svenska utlandsmyndigheter.

Dataskyddsförordningen är tillämplig även för personuppgiftsansvariga och personuppgiftsbiträden som inte alls är etablerade inom EU, om behandlingen avser registrerade i unionen och har anknytning till antingen utbjudande av varor eller tjänster till registrerade i unionen eller övervakning av registrerades beteende i unionen. Enligt dataskyddsförordningen gäller således i dessa fall effektlandsprincipen. Det framstår som lämpligast att den nationella regleringen utgår från samma princip när det gäller personuppgiftsansvariga och personuppgiftsbiträden som inte är etablerade inom EU. Detta innebär att dataskyddslagen i sådana fall bör gälla vid behandling av personuppgifter som avser registrerade som befinner sig i Sverige, om behandlingen har anknytning till antingen utbjudande av varor eller tjänster till registrerade i Sverige eller övervakning av registrerades beteende i Sverige.

Samma åldersgräns för samtycke bör gälla för alla barn som bor i Sverige

Dataskyddsutredningen har föreslagit att barn som har fyllt 13 år själva ska kunna lämna samtycke till behandling av personuppgifter vid erbjudande av informationssamhällets tjänster. För det fall att det ska föreskrivas en åldersgräns som avviker från dataskyddsförordningens, bör en sådan bestämmelses tillämpningsområde inte följa etableringslandsprincipen. I annat fall skulle det kunna leda till olika åldersgränser för barn i Sverige beroende på vilken åldersgräns som valts i tjänsteleverantörens etableringsland. Det skulle också kunna leda till otillbörliga lättnader för företag och organisationer som är etablerade i Sverige och som riktar sig till barn i andra länder. Dessutom vore det olämpligt av Sverige att införa en sänkt åldersgräns som skulle kunna åberopas vid personuppgiftsbehandling avseende barn i andra medlemsstater, där lagstiftaren gjort en annan bedömning av sakfrågan.

Mot denna bakgrund bör en eventuell bestämmelse om barns samtycke gälla vid behandling av personuppgifter som avser barn som bor i Sverige, oavsett var de personuppgiftsansvariga eller deras biträden är etablerade.

Förslag till lag (2018:xx) med kompletterande bestämmelser till EU:s dataskyddsförordning

Nuvarande lydelse enligt SOU 2017:39	*Föreslagen lydelse*
	1 kap.
	1a §
	Denna lag gäller vid behandling av personuppgifter som utförs av personuppgiftsansvariga eller personuppgiftsbiträden som är etablerade i Sverige, om behandlingen utförs inom ramen för verksamhet som bedrivs vid verksamhetsställen här i landet. Lagen gäller även vid behandling av personuppgifter som utförs av personuppgiftsansvariga som inte är etablerade i Sverige, men på en plats där svensk rätt gäller enligt folkrätten.
	Lagen gäller också vid behandling av personuppgifter som avser registrerade som befinner sig i Sverige och som utförs av personuppgiftsansvariga eller personuppgiftsbiträden som endast är etablerade i tredjeland, om behandlingen har anknytning till
	1. utbjudande av varor eller tjänster till registrerade i Sverige, eller
	2. övervakning av registrerades beteende i Sverige.
	Bestämmelsen i 2 kap. 2 § gäller vid behandling av personuppgifter som avser barn som bor i Sverige, oavsett var de personuppgiftsansvariga eller deras biträden är etablerade.

Förteckning över remissinstanserna (Kompletterande promemoria)

Remissvar har lämnats av Riksdagens ombudsmän, Svea hovrätt, Hovrätten för Västra Sverige, Södertörns tingsrätt, Kammarrätten i Stockholm, Kammarrätten i Göteborg, Kammarrätten i Jönköping, Förvaltningsrätten i Stockholm, Förvaltningsrätten i Malmö, Förvaltningsrätten i Jönköping, Förvaltningsrätten i Linköping, Justitiekanslern, Säkerhetspolisen, Säkerhets- och integritetsskyddsnämnden, Datainspektionen, Kommerskollegium, Försvarsmakten, Försvarets radioanstalt, Socialstyrelsen, Barnombudsmannen, Verket för innovationssystem, Konsumentverket, Myndigheten för ungdoms- och civilsamhällesfrågor, Uppsala universitet, Lunds universitet, Göteborgs universitet, Umeå universitet, Kungliga tekniska högskolan, Karolinska institutet, Post- och telestyrelsen, Konkurrensverket, Regelrådet, Statens medieråd, Almega, Sveriges advokatsamfund, Sveriges Akademikers Centralorganisation och Swedish Direct Marketing Association.

Umeå tingsrätt, Tillväxtverket, Örebro universitet, Barnens rätt i samhället, Civil Rights Defenders, Forum för dataskydd, Företagarna, IT&Telekomföretagen, Landsorganisationen i Sverige, Svensk Handel, Teknikföretagen, Sveriges konsumenter, Småföretagarnas riksförbund, Surfa lugnt, Svenska avdelningen av Internationella juristkommissionen, Svenska journalistförbundet, Svenska sektionen av Amnesty International, Svenskt Näringsliv, Tidningsutgivarna och Tjänstemännens centralorganisation har avstått från att lämna synpunkter på förslagen i promemorian eller har inte svarat på remissen.