dataskydd.net

ORG.NR 802495-4797 – HTTPS://DATASKYDD.NET – INFO@DATASKYDD.NET

Dataskydd.net Sverige
Alsnögatan 18
116 41 Stockholm

Justitiedepartementet
103 33 Stockholm

Örsundsbro 2017-10-27

Remissyttrande över En omarbetad domstolsdatalag – Anpassning till EU:s dataskyddsförordning – Ds 2017:41 Ju2017/06965/DOM

Dataskydd.net är en svensk ideell, partipolitiskt obunden förening som verkar för bättre tekniskt och juridiskt dataskydd för privatpersoner i Sverige. Det här dokumentet är publicerat med licensen CC0.

Dokumentet börjar med en sammanfattning där tillstyrkanden och avstyrkanden listas per kapitel i promemorian där förslagen förekommer. Sedan följer särskild behandling av koncept i den europeiska dataskyddslagstiftningen som promemorian, i vår mening, missförstått eller stridit emot. Sedan följer kommentarer på var och en av förslagen till lagändringar och till sist har vi inkluderat en källförteckningar med webblänkar där möjligt.

Innehållsförteckning:

Sammanfattning av förslag

Sammanfattning.

Tillstyrker förslag: Domstolsdatalagen 2 §, 3 §, 3a §.

Avstyrker delvis förslag: Domstolsdatalagen 5a §, 10 §, 17 §, 17a §. Förordningen om vattenverksamhet 8 §. Förordningen om miljöfarlig verksamhet och hälsoskydd 48a §.

Avstyrker förslag: Domstolsdatalagen 4 §, 5 §, 7 §, 10 §, 11 §, 13 §, 14 §, 19 §, 19a §, 20 §, 22 §. Domstolsdataförordning 3 §, 4 §, 5 §, 11b §, 14 §.

Det är uppenbart att promemorian är skriven utifrån ambitionen att förändra så lite som möjligt.[1] Dataskyddsförordningen är dock mycket tydligare än tidigare europeisk lagstiftning om behovet av proportionalitetsbedömningar, och innehåller nya regler till skydd för enskilda innefattandes högre krav på konsekvensbedömningar, säkerhetsåtgärder och information till enskilda.[2] De föreslagna reglerna blir inte begripliga för de som reglerna tillämpas på (det vill säga domstolar) om regeringskansliet bortser ifrån de nya kraven. Särskilt blir reglerna inte begripliga för *enskilda registrerade*, som ju tillhör gruppen av aktörer som reglerna ska vara begripliga för. Domstolsdatalag är, som Dataskydd.net tidigare påtalat,[3] skriven enligt en föråldrad, svensk integritetsskyddssystematik, som inte faktiskt skyddar integriteten. Lagen tillkom under en period då regeringen i stället borde ha anpassat denna föråldrade systematik efter EU:s dataskyddsrätt i stället för att fräsa iväg för sig själv. Att den föråldrade systematiken för svenska registerförfattningar inte skyddar integriteten har etablerats av

Vanliga svenskar. Enskilda privatpersoner som befinner sig i Sverige tillhör den grupp av aktörer som berörs av och som behöver kunna förstå vilka rättigheter de har enligt dataskyddslagstiftningen. Dataskydd är en grundläggande rättigheter och ska som sådan kunna utövas effektivt. Fokuset i registerförfattningarna behöver alltså i högre utsträckning än vad som är fallet fokusera på förutsebarhet och nytta för enskilda privatpersoner, inte bara på hur enskildas rättigheter ska åsidosättas.

Bild: Stickande kulla av Anders Zorn, 1901 (kulturallmänningen).

[1] Ds 2017:41, s. 17

För att anpassa domstolsdatalagen till det nya regelverket för personuppgiftsbehandling föreslår vi att lagen endast ska gälla för sådan behandling av personuppgifter som omfattas av dataskyddsförordningens tillämpningsområde. I övrigt innebär vårt förslag att lagens tillämpningsområde ska kvarstå oförändrat[.]

Ds 2017:41, s. 18:

Någon förändring av lagens befintliga ändamålsbestämmelser föranleds /.../ inte[.]

Ds 2017:41, s. 19:

[*B*]*estämmelserna om behörighetsbegränsningar, personuppgiftsansvar, utlämnande av personuppgifter på medium för automatiserad behandling*[*, behandling av känsliga uppgifter*] *och direktåtkomst att kunna kvarstå oförändrade.*

Ds 2017:41, s. 56:

För den del av verksamheten som faller inom dataskyddsförordningens tillämpningsområde bör domstolsdatalagen enligt vår bedömning i materiellt hänseende snarare kvarstå oförändrad i så stor utsträckning som möjligt.

[2] *Se t. ex.* Datainspektionen, Dnr 1015-2017 med kommentarer på förslaget om en omreglerad spelmarknad:

För att kunna svara på frågan om ett författningsförslag är förenligt med reglerna om skydd för den personliga integriteten i grundlagarna och EU-rätten behöver man göra en integritetsanalys. En integritetsanalys ska särskilt svara på frågan om konsekvenserna för den personliga integriteten som en föreslagen personuppgiftsbehandling medför är proportionerliga i förhållande till det man avser att uppnå med behandlingen. I detta ingår att bedöma om behandlingen av personuppgifter är nödvändig utifrån de avsedda ändamålen med behandlingen och om det finns alternativ som är mindre integritetskänsliga. En förutsättning för en sådan analys är en noggrann kartläggning och beskrivning av den föreslagna personuppgiftsbehandlingen och en analys av vilka konsekvenser för den personliga integriteten som behandlingen medför eller kan medföra.

[3] Se Dataskydd.net:s kommentarer till riksdagen om Prop. 2014/15:148 om en ny domstolsdatalag.

två på varandra följande större översyner av svenskt integritetsskydd, den senaste av vilken avslutade bara under sommaren 2017.[4]

Som redan påtalats av utredningen om en ny brottsdatalag har det skett en sammanblandning mellan vad som i dataskyddsrättslig mening är särskilt bestämda ändamål och tillåtna rättsliga grunder för behandling.[5]

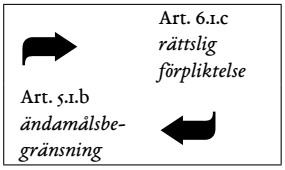
Många av problemen i svenska registerförfattningar kommer sig att regeringskansliet inte gör någon stark åtskillnad mellan den *rättsliga grunden för behandlingen* (art. 6, dataskyddsförordningen) och *ändamålsbegränsning* (art. 5.1.b).

Ändamålsbegränsning är något som den personuppgiftsansvarige gör och är ansvarig för. Myndigheter får alltså uppdrag av regeringen (rättsliga förpliktelser, uppdrag att ägna sig åt myndighetsutövning och så vidare) som kan kräva personuppgiftsbehandling. Myndigheterna ska då begränsa behandlingen av personuppgifterna till det som ändamålet (att uppfylla sina förpliktelser eller genomföra sitt uppdrag) kräver. Genom insyn, transparens och dokumentation ska privatpersoner ger goda förutsättningar att hävda sina rättigheter enligt förordningen. Domstolsdatalag sätter denna ansvarutkrävandekedja ur spel genom att dels avhända myndigheterna deras ansvar att vara restriktiva med personuppgiftsbehandlingen, och dels avhända privatpersoner möjligheter till utövande. Det uppstår cirkelresonemang.

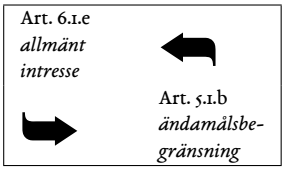
För företag fungerar dynamiken mellan artikel 5 och artikel 6 tvärtom: företag kan komma på ett ändamål, som ska vara begränsat, och behöver sedan ta reda på vilken rättslig grund som krävs för att ändamålet ska vara giltigt.

Dataskydd.net är inte övertygade om att det invecklade systemet i Sverige med särskilda registerförfattningar bäst tillgodoser privatpersoners och samhällets behov av ett starkt integritetsskydd. Tvärtom riskerar de att göra det svårt för privatpersoner att förutse vilket skydd de har, och myndigheterna distraheras från de proportionalitetsbedömningar och säkerhetsavvägningar de ska göra inför varje insamling och behandling av privatpersoner. Dessutom verkar registerförfattningssystemet ha lett till stora svårigheter för regeringskansliet att utvärdera och förstå hur enskildas integritet skyddas ute i myndigheternas verksamheter. Regeringskansliet blir extra känsligt för påverkansarbete från de myndigheter som har bäst insikt i speciallagarna som gäller för den egna verksamheter, medan privatpersoner hamnar i extra svag ställning att nå både regeringskansliet, myndigheterna och till sist kunna utöva sina rätithgeter.

1. Ändamålet är lagstadgat, därför förpliktigar det.



2. Ändamålet är lagstadgat, därför är det ett allmänt intresse.



Cirkelresonemang (exempel).

SparL har i 3 § punkt 2 en ändamålsbegränsning utan juridisk bas. Det vill säga, ändamålet med Skatteverkets personadressregister anges vara att kunna ta ut uppgifter om namn och adress genom urvalsdragning för direktreklam, opinionsbildning eller samhällsinformation eller annan därmed jämförlig verksamhet. Ändamålsbegränsningen uppfyller förvisso kraven i dataskyddsförordningens artikel 5.1.b (*ändamålsbegränsning*) men det är inte uppenbart vilka villkor i dataskyddsförordningens artikel 6 som åberopas för behandlingen i 3 § punkt 2. Är det ett allmänt intresse att Skatteverket kan behandla uppgifter för att lämna ut dem till direktreklamföretag (artikel 6.1.e)? Eller är det en rättslig förpliktelse för Skatteverket att tillhandahålla urvalsdragna personuppgifter för opinionsbildning och samhällsinformation (artikel 6.1.c)? Förordning (2007:780) med instruktion för Skatteverket anger inte att Skatteverket skulle ha några sådana rättsliga förpliktelser, och inte heller regleringsbrevet antyder att Skatteverket skulle ha förpliktelser gentemot varesig opinionsbildare eller reklammakare.

[4] SOU 2016:41, kap. 3.3, SOU 2008:3, s. 13–14. Ref. också SOU 2017:52.

[5] SOU 2017:29, s. 240–241.

Informationshanteringsutredningen anser att det har skett en sammanblandning mellan vad som i dataskyddsrättslig mening är särskilt bestämda ändamål och tillåtna rättsliga grunder för behandling. Det finns enligt den utredningen risk att tillämparen blandar samman ändamål med rättslig grund och godtar ett i författning bestämt allmänt ändamål som ett särskilt och tillräckligt preciserat ändamål och drar den felaktiga slutsatsen att personuppgiftslagens krav därmed är uppfyllda. /.../

Utredningen anser att det finns fog för Informationshanteringsut- redningens uppfattning att vad som i dataskyddsrättslig mening är tillåtna rättsliga grunder för behandling och vad som är renodlade ändamålsbestämmelser ibland har blandats samman. En sådan sammanblandning kan leda till att tillämparen förväxlar rättslig grund med ändamål och godtar ett i författning angivet allmänt ändamål som ett särskilt och tillräckligt preciserat ändamål. Det är därför viktigt att det görs tydligare skillnad mellan bestämmelser om rättslig grund och ändamålsbestämmelser.

Registerförfattningsbestämmelser

I det nedanstående har Dataskydd.net framställt ett antal begrepp och underligheter som förekommer i svenska registerförfattningar, och som synbart gör väldigt lite för att förbättra eller förenkla möjligheter för privatpersoner att utöva sina rättigheter till privatliv och dataskydd. Domstolsdatalag innehåller samtliga dessa specialbegrepp.

Direktåtkomst

Direktåtkomst föreslås ofta vara ett kostnadseffektivt sätt att möjliggöra större informationsdelning mellan myndigheter, särskilt om det upplevs att kontrollåtgärder mot tjänstemän eller privatpersoner behöver utökas.[6] Kontrollåtgärder som riktas mot individer, som individer inte har någon möjlighet att värja sig emot eftersom deras normala dataskyddsrättigheter sätts ur spel, är dock integritetskränkande även om de är billiga att genomföra. Att bevara systematiken för lagstadgad direktåtkomst kan vara önskvärt, eftersom det inför en extra bromskloss som gör att onödiga integritetskränkningar inte uppstår i onödan. För att inte i onödan begränsa privatpersoners rättigheter bör det dock framgå i direktåtkomstbestämmelser att dataskyddsförordningen artikel 14 (*information till enskild*) och artikel 25 (*inbyggt integritetsskydd*) gäller. Det viktiga är alltså privatpersoner kan informeras om hur uppgifter om dem själva använts, att detta loggas, och åtkomstmekanismerna upprätthåller integritet och informationssäkerhet.

Uppgiftskategorier

Att särreglera vilka uppgiftskategorier som ska ingå i en viss databas är inte lika nödvändigt. Dataskyddsförordningen artikel 5.1.c (*dataminimering*) bör redan medföra att inget register upprättas som innehåller fler uppgiftskategorier än vad som är nödvändigt för att uppnå syftet med behandlingen, och när ett register väl är på plats är det tillräckligt dyrt och komplicerat att ändra på registrets struktur för att man inte ska behöva anta att den extra trögheten det innebär att ha en lagstiftning om kategorierna är nödvändig. Konsekvensbedömningar och information till privatpersoner är i sådana fall bättre verktyg att säkerställa återhållsamhet i registreringsverksamheten.

Känsliga uppgifter

Dataskyddsförordningen artikel 9.2 innehåller redan en uttömmande lista på tillfällen då känsliga uppgifter kan behandlas, varför det inte är nödvändigt att införa särskilda lagstöd för sådan behandling. Förordningens 5.1.b (*ändamålsbegränsning*), artikel 5.1.c (*dataminimering*) och 5.1.e (*lagringsminimering*) borde redan få myndigheterna att i egenskap av personuppgiftsansvariga inte behandla uppgifterna annat än om det är absolut nödvändigt. Enskildas rättigheter i artiklarna 12–22 samt tillsynsverksamhet förhindrar att myndigheterna behandlar känsliga uppgifter i allt för hög utsträckning.

Gallring

Gallring ska ske så fort uppgifterna inte längre behövs enligt dataskyddsförordningen artikel 5.1.e (*lagringsminimering*). Genom att fixera tidsbegränsningar i registerförfattningar som inte är korrelerade med uppgifternas användningsområden i myndigheternas verksamhetsinstruktioner riskerar regeringen att försämra snarare än förbättra

[6] Jfr RiR 2010:18.

Tidigare i Dataskydd.net:s serie av remissyttranden om registerförfattningar, i de avseenden det har beröringspunkter med innevarande promemoria:

1. SOU 2017:29: särskilt avseende insyn och informationssäkerhet, samt tillsyn.

2. SOU 2017:39: särskilt om begreppsfrågor (pseudonymisering, allmänt intresse), arkiv, insyn och informationssäkerhet, samt tillsyn.

3. Fi2017/02899/S3: särskilt om begreppsfrågor (allmänt intresse), rättslig grund (art. 6) visavi dataskyddets principer (art. 5).

4. Ds 2017:26: särskilt om allmänt intresse och privat sektor.

5. Ds 2017:33: särskilt om rättslig grund (art. 6) visavi dataskyddets principer (art. 5).

Samtliga remissyttranden återfinns på https://dataskydd.net/vara-remissvar

	enskildas integritetsskydd. Motsvarande resonemang gäller som för känsliga uppgifter.
Personuppgiftsansvar	Vem som ska vara ansvarig för behandlingar kan behöva framgå av lagstiftning, för att göra ansvaret tydligt för enskilda och för myndigheterna själva.
Sökbegrepp	Sökbegreppsbegränsningar är ett sorts krav på användargränssnitten för tjänstemäns åtkomst till vissa databaser, och följer per automatik från dataskyddsförordningen artikel 25 (*inbyggt integritetsskydd*).[7] Sökbegränsningarna motiveras i vissa fall sekundärt med att det krävs specifika begränsningar av offentlighetsprincipen enligt tryckfrihetsförordningen,[8] med motiveringen att de, eftersom de förbjuder myndigheterna att upprätta vissa sorters handlingar som annars skulle gå att upprätta vid förfrågan, höjer integritetsskyddet. Om detta senare är målet med sökbegränsningsparagraferna, borde det vara enklare och mer transparent att skriva om dessa regler som förbud mot att upprätta handlingar av det slag som avses, istället för att ge paragraferna funktionen av specifikation för användargränssnitt.

Domstolsdatalag: de avstyrkta paragraferna

Dubbel lag är bättre lag? Domstolsdatalag 6 §, 7 §, 10–11 §§, 19–22 §§

Promemorians förslag till domstolsdatalag 6 §, 7 §, 10–11 §§, 19–22 §§ behövs inte. Dessa bestämmelser finns redan i förslaget till ny dataskyddslag eller direkt i EU:s dataskyddsförordning. Man behöver inte återupprepa samma lagtext om och om igen. Domstolsverket styrs av juridiskt tränade individer som redan har förmågan att förstå den lagtext som redan finns. Ingenting blir klarare av dubbel lagstiftning.

Otydligt syfte med lagen? Domstolsdatalag: 14 §, Domstolsdataförordning: 3–5 §§

Bestämmelserna om sökbegränsningar i Domstolsdatalag: 14 §, Domstolsdataförordning: 3–5 §§ försämrar privatpersoners rättigheter att förstå och utöva sina rättigheter, i och med det att de sannolikt har ett annat syfte än de utger sig för att ha. Medan bestämmelserna utformas som en specifikation för användargränssnitt, handlar de i själva verket om att begränsa möjligheten att upprätta allmänna handlingar (i alla fall presumtivt). Regeringskansliet bör åtgärda dessa

[7] *Se t. ex.* Datainspektionen. Inbyggt integritetsskydd, 2012.

[8] *Se t. ex.* SOU 2017:39, s. 176:

> *Ett sådant sökförbud innebär i svensk rätt också att offentlighetsprincipen inskränks enligt den så kallade begränsningsregeln i 2 kap. 3 § tredje stycket tryckfrihetsförordningen. En begäran att få tillgång till en sammanställning av uppgifter som är resultatet av en sådan förbjuden sökning ska alltså avslås på den grunden att sammanställningen inte anses förvarad hos myndigheten. Att sammanställningar av känsliga personuppgifter inte lämnas ut framstår som en inte obetydlig integritetsvinst för de registrerade. Det bör dock understrykas att begränsningsregeln inte hindrar att sökningar görs i färdiga elektroniska handlingar vid en begäran om tillgång till allmänna handlingar. Sökning får alltså på begäran ske i upptagningar där myndigheten eller den som lämnat in handlingen till myndigheten har gett upptagningen ett bestämt, fixerat, innehåll som går att återskapa gång på gång.*

förväxlingsmöjligheter och klargöra vad de egentligen avser, innan de framställer något förslag till riksdagen.

Särlagstiftning är lika med färre förpliktelser? Domstolsdatalag 17–17a§§, Domstolsdataförordning 11b §, 14 §

Genom att särlagstifta om direktåtkomst i Domstolsdatalag 17–17a§§, Domstolsdataförordning 11b §, 14 § fråntar regeringskansliet Domstolsverket och tillhörande organ skyldigheten att på ett korrekt sätt logga och hålla rätt på åtkomster till uppgifter i verkets register. Det följer nämligen av de vanliga bestämmelserna för utlämnande av uppgifter i dataskyddsförordningen att det ska vara möjligt för individer att förstå hur deras uppgifter lämnas ut och skickas vidare mellan olika verksamheter.

Men vad gäller egentligen? Domstolsdatalag 4–5 §§

Särbestämmelser i registerförfattningar, i den utsträckning registerförfattningar alls ska finnas, bör begränsas till ett minimum. Systematiken bakom 4–5 §§, och domstolsdatalag i övrigt, är den motsatta: särreglera så mycket som möjligt. Innebörden av 4–5 §§ skulle mycket enklare kunna uttryckas som att dataskyddsförordningen och dataskyddslag med kompletterande bestämmelser gäller om ingenting annat framgår av domstolsdatalag (det vill säga, samma sorts kortfattade beskrivning som ges i 3a §). I stället väljer utredaren att göra långa uppräkningar av paragrafer, vilket får det att framstå som om att allt som inte är med på listan inte gäller (och därför inte behöver tas i beaktande av personuppgiftsansvarig). Detta är fel, eftersom dataskyddsförordningen de facto gäller.

Mark- och miljödomstolar (två lagförslag)

Särskilda bestämmelser om utlämnande av uppgifter från Mark- och miljödomstolar är onödiga. Antingen följer utlämnandet av en befintlig uppgift som domstolen har (det vill säga, det finns en rättslig grund enligt artikel 6, dataskyddsförordningen), och då ska utlämnnandet ske med förordningens bestämmelser om insyn för enskilda, säkerhet och övrigt i beaktande. Eller så följer utlämnandet inte av en befintlig uppgift som domstolen har.

Eller så är utlämnandet av uppgifter begränsat i offentlighets- och sekretesslagen, och då är det offentlighets- och sekretesslagen man behöver ändra.

Det grötiga gyttret av specialbestämmelser gör den samlade massan av svenska personuppgiftslagar och integritetsskydd svåröverskådlig, vilket inte hjälper enskilda privatpersoner och inte heller hjälper dem som ska följa lagarna (annat än om de hittar sätt att utnyttja det grötiga gyttret på sådant sätt att de slipper upprätthålla god transparens och insyn mot medborgarna, eller slipper upprätthålla god informationssäkerhetsnivå).

EU-domstolen och stadgan: var är svensk rätt?

Så vitt vi förstår återstår problemet att lösa hur de svenska registerförfattningarna ska anpassas efter EU-domstolens praxis, och särskilt domstolens tolkningar av dataskyddsförordningen eller dataskyddslagstiftning mot bakgrund av EU:s

stadga för grundläggande rättigheter.[9] Eftersom dessa nya rättsförhållanden i princip borde innebära att Sverige har något liknande en konstitutionsdomstol på dataskyddsområdet, behöver både regeringen, dess tjänstemän och lagstiftaren i riksdagen förbereda sig på att man inte på samma sätt som tidigare trivialt kan åsidosätta enskildas rättigheter.

Den direkta tillämpningen av dataskyddsförordningen i Sverige innebär att EU-domstolens uttalanden om dataskyddsförordningens innebörd även gäller för svenska myndigheter och registerförfattningar. Det kan till exempel röra omfattningen av enskildas rättigheter eller möjligheten för myndigheter att hitta nya ändamål för redan insamlade uppgifter enligt förordningens artikel 6.4.

Svensk lagstiftning kan i och med ovanstående omständigheter komma att påverkas av rättstvister som uppstått i ett annat medlemsland. Till exempel sådana länder där privatpersoner och organisationer, till skillnad från i Sverige, har möjlighet att efterfråga rättslig prövning av lagstiftning eller där det är enklare att utkräva tjänstemannaansvar eller direkt ansvar av myndigheter.

Utredningens långa uppehåll på begreppet *dömande verksamhet*[10] visar att det redan finns insikter om att EU-rätten faktiskt kan komma att påverka, eller behöva påverka, hur dataskyddet utvecklas i Sverige – så se till att det finns en process för att hantera det! Regeringskansliet är ett vuxet kansli med långa anor, inget dagisbarn i en sandlåda som tappat bort sin spade. Regeringskansliet bör inte försätta sig i situationen att det riskerar bli överrumplat av en föränderlig värld, utan ha tillräckligt med kompetens och framförsikt för att ha planerat i förväg.

Viktigt för enskilda att få reda på säkerhetsfel

Rapporter om personuppgiftsincidenter direkt till privatpersoner redan obligatoriska för företag och myndigheter i 47 amerikanska delstater.[11] I åtta av delstaterna publiceras incidentrapporterna direkt på webben för hela världen att skåda. Den ekonomiska teorin bakom offentliggörandet är att företag och myndigheter som tvingas stå till svars för sina säkerhetsproblem har starkare incitament att ha goda säkerhetsrutiner och åtgärda säkerhetsproblem som upptäcks.[12] Om det istället är möjligt att hemlighålla säkerhetsproblem kan starka drivkrafter som viljan att slippa ta en kostnad, eller viljan att slippa bli generad, leda företag och myndigheter att inte åtgärda säkerhetsproblemen. Dataskydd.net har beskrivit problemet i ett antal tidigare inlagor och remissyttranden.[13]

Transparens kring säkerhetsproblem hjälper företag och myndigheter att förvissa konsumenter och medborgare om att de tar säkerhetsproblem på allvar.[14]

I motsats till den individcentriska incidentrapporteringen finns ingen särskilt väl underbyggd ekonomisk teori bakom EU-ländernas preferenser för inci-

Amerikanska delstater med offentligt publicerade incidentrapporter:

- Iowa
  https://www.iowaattorneygeneral.gov/for-consumers/security-breach-notifications/
- Kalifornien
  https://oag.ca.gov/ecrime/databreach/list
- Maryland
  http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/breachnotices.aspx
- Montana
  https://dojmt.gov/consumer/consumers-known-data-breach-incidents/
- New Hampshire
  http://www.doj.nh.gov/consumer/security-breaches/
- Oregon
  https://justice.oregon.gov/consumer/databreach/
- Vermont
  http://ago.vermont.gov/focus/consumer-info/privacy-and-data-security1/data-security-breaches/archived-security-breaches.php
- Washington
  http://www.atg.wa.gov/data-breach-notifications

Incidentrapporterna publiceras på Attorney Generals webbplats och går att beskåda av både invånare i delstaten, forskare och andra företag.

[9] Europeiska unionens stadga om de grundläggande rättigheterna, Europeiska unionens officiella tidning nr C 083 , 30/03/2010 s. 0389 – 0403.

[10] Ds 2017:41, kap. 8

[11] National Conference of State legislatures. Security Breach Notification Laws. [http://perma.cc/7EDG-KVBF].

[12] ENISA. 2008. Security Economics and the Internal Market. Författare: Ross Anderson, Rainer Boehme, Richard Clayton, Tyler Moore.

[13] *Se bl. a.* Dataskydd.net:s remissyttrande över SOU 2015:23 om informationssäkerhet, SOU 2017:36 om informationssäkerhet, SOU 2016:41 om dataskydd, och Ju2017/02002/L4 om ett tekniskt sensorsystem.

[14] Deloitte, Deloitte Australian Privacy Index 2015: Transparency is opportunity.

dentrapporter till myndigheter. Betydligt kraftigare ekonomiska sanktioner och mer övervakning av privat sektor skulle, enligt två österrikiska säkerhetsekonomer, behövas för att systemet med incidentrapporter till myndigheter, i syfte att hjälpa myndigheterna utarbeta riktlinjer, ska kunna ha chans att vara effektivt ur säkerhetshöjande perspektiv.[15]

Följande historia från det svenska företaget Ericsson, återberättad av Per Göran Ohlsson, Hans Blackman och Jan Svensson, kan tjäna som exempel för vitsen med transparens kring säkerhetsfel:

> Våren 1998 hände något som kunde fått dramatiska konsekvenser för Ericsson och kanske för hela mobiltelefonbranschen. I mitten av maj kom en rapport om att en HotLine Combi den 25 maj hade exploderat i en trädgård i Arlöv. /.../ Samtidigt kom information om en ny explosion i Värmland. /.../
>
> Enligt uppgift ska Ericssonledningen ha tvekat om vad som skulle göras, men Nils Rydbeck krävde att alla telefoner skulle återkallas[. E]n annonskampanj den 31 maj gick ut med budskapet: ”Vi måste få låna din HotLine en stund”.
>
> Ericsson Radios serviceverkstäder hade kvällsöppet till klockan åtta hela följande vecka. Man lödde om litiumbatterier och ökade avståndet mellan batteri och ledare. En kvällstidning lär ha försökt göra reportage med en av de drabbade, men denne vägrade (kanske för att han fått ett nytt golfset som kompensation) och hela historien slutade lyckligt. Ericsson fick stor goodwill för sitt agerande – snabb och effektiv åtgärd utan extra kostnad för kunden och med generösa öppettider. *Det sägs att konkurrenten Mobira (alltså Nokia) anklagade Ericsson för att ha hittat på hela historien för att få publicitet.*
>
> – Ericssons mobiltelefoner 1983–2001, s. 25–26.[16]
>
> [vår italisering]

Kontinuerligt kretslopp. Dataskydd är något som måste säkerställas genom att hela organisationen har en integrerad process för att åstadkomma dataskydd. Det behöver inkludera både leverantörer, beställare, organisatoriska omständigheter och verksamheten.

Bild: CC0 recycling.com.

NJA PSEUDONYMISERAR

Pseudonymisering sker i Nytt juridiskt arkiv och de prejudicerande beslut som tillgängliggörs på dom.se. Denna sorts pseudonymisering blir mindre explicit uppmuntrad av att utredaren inte föreslår göra det lätt för myndigheterna att redan från början arkivera sina handlingar enligt denna modell. Dataskyddet borde ses som ett kretslopp, där alla komponenter är viktiga.

Arkiv och statistik

Pseudonymisering

Utredningen har förbisett möjligheten att använda pseudonymer i allmänna handlingar som ska arkiveras eller användas som statistiskt underlag. Pseudonymisering innebär att tröskeln för att koppla en specifik handling till en specifik individ blir högre. Integritetsskyddet blir därför högre. Vidareanvändning av det arkiverade materialet i forskning eller statistikframställning blir mindre integritetskränkande, samtidigt som insynen i myndigheternas verksamheter inte behöver begränsas.

God dataskyddspraktik behövs i hela värdekedjan för databehandling, vilket reflekterats i den europeiska lagstiftningen och därför bör föras in även i den svenska implementationen. Den nyligen publicerade Digitaliseringsstrategin[17] bekräftar att regeringen är motiverad att säkerställa sig om god dataskyddspraktik i hela värdekedjan, och till och med sikta på att bli drivande på området.[18] Den ansträngningen börjar med att man inte gör lättsamma förbiseenden i Dataskyddslag.

[15] Stefan Laube (University of Münster), Rainer Böhme (University of Innsbruck), The Economics of Mandatory Security Breach Reporting to Authorities, presenterad vid The Workshop on the Economics of Information Security, 22–23 juni 2015 i Delft, Nederländerna.

[16] Per Göran Ohlsson, Hans Blackman och Jan Svensson, Ericssons mobiltelefoner 1983–2001, Roos & Tegnér förlag, 2015. Tryckt i Pozkal, Inowrocław, Polen.

[17] Regeringen, För ett hållbart digitaliserat Sverige – en digitaliseringsstrategi (N2017/03643/D).

[18] *Ibid.*, s. 18–19.

Rätten till rättelse

Redan 1972 observerades att blotta vetskapen om att felaktiga uppgifter om den egna personen finns registrerade hos en myndighet kan skapa stort obehag för en enskild.[19] Det rör inte bara risken att uppgifterna åter tas i bruk[20] och därmed riskerar användas som grund för beslut eller åtgärder mot den egna personen, utan också oron för att en genomgång av de arkiverade handlingarna medför att man blir offer för förutfattade meningar.

Logiken bakom att ha en rätt till rättelse i lagstiftningen är alltså från början klar: det ska skydda privatpersoner från obehaget det innebär att felaktigt utpekas som något man inte är. Samtidigt är logiken bakom att spara felaktiga uppgifter svårbegriplig.

> Datainspektionen har redan för ett decennium sedan kritiserat Försäkringskassan för deras bristande rutiner för rättelse av felaktiga uppgifter.[21] Påpekandena om brister verkar inte ha utmynnat i åtgärder mot att Försäkringskassan inte rättar felaktiga uppgifter, men däremot förefaller en utbredd uppfattning ha slagit rot i utredningsväsendet att rätten till rättelse som sådan är problemet, för att rätten till rättelse kan medföra att myndigheter behöver vidta åtgärder.[22] Informationshanteringsutredningen föreslog till exempel skarpa begränsningar av rätten till rättelse.[23]

Myndigheterna gagnas inte av att ha felaktig information om en privatperson. Forskningen kan inte antas ha nytta av att det finns felaktigheter i forskningsunderlaget. Tvärtom borde forskning gagnas mycket mer av att forskningsunderlaget är korrekt. Allmänheten har inte heller något intresse, annat än möjligen nyfikenhet, av att ta del av felaktiga uppgifter om en enskild privatperson. Anledningen till att det verkar finnas en stark rörelse för bevarande av felaktiga uppgifter i svenska myndighetsregister kan istället vara en annan: det är dyrt och tråkigt att förändra tekniska system och organisatoriska rutiner.

Ångestskapande. Blotta vetskapen om att det finns felaktiga uppgifter som kan komma att utgöra grund för nya beslut, bli föremål för forskning eller komma till eftervärldens vetskap kan bli en stor, ångestskapande börda för privatpersoner. Förutom att det påverkar den enskildes förtroende för statsmakten negativt, kan det också medföra att privatpersonen av rädsla inte fungerar bland sina medmänniskor.
Bild: CC0 https://TheNounProject.com

---

[19] SOU 1972:47, s. 87–88.

> *Varje felaktighet i personuppgifter som ingår i ett personregister kan befaras medföra otillbörligt integritetsintrång. På grund av de möjligheter som den automatiska databehandlingen ger att använda en uppgift i många olika sammanhang och att finna den även efter lång tid är riskerna för att en oriktighet skall vålla skada större än i fråga om manuellt hanterade uppgifter. Härtill kommer att den omständigheten att en uppgift härrör från ett ADB-register i mångas ögon ger den ett särskilt sken av riktighet och objektivitet. Skulle det finnas skäl att misstänka, att en uppgift är oriktig, bör registerföraren därför vara skyldig att kontrollera den. Detta torde f. ö. i regel ligga även i hans eget intresse. Visar det sig att uppgiften är felaktig, bör registerföraren vara skyldig att rätta den. Kan uppgiften inte bestyrkas, bör den utgå ur registret om den registrerade påyrkar det.*

[20] *Jfr*. förslagen i SOU 2017:39, kap. 14.4.2.

[21] Datainspektionen Dnr 998-2007 Beslut [mot Försäkringskassan] efter tillsyn enligt personuppgiftsiagen (1998:204):

> *Det finns inom Försäkringskassan några dokument som beskriver när och hur handläggare ska beställa information till den registrerade (s.k. registerutdrag) ur Försäkringskassans system. Det finns dock inget dokument som behandlar gränsdragningen mellan partsinsyn, offentlighetsprincipen och registerutdrag. Det saknas helt och hållet dokument om Försäkringskassans rättelsemöjligheter.*
>
> *Försäkringskassan har således ännu inte tagit fram den enhetliga rutin för rättelser som Försäkringskassan i samband med Datainspektionens tidigare inspektion i december år 2005 (dnr 1857-2005) planerade att genomföra.*

Någon uppföljande tillsyn verkar inte ha skett efter 2007, och det är oklart huruvida det idag finns rutiner på Försäkringskassan för rättelse av felaktiga uppgifter.

[22] SOU 2015:39, s. 556.

[23] *Se även* Dataskydd.net:s remissyttrande över SOU 2015:39 Myndighetsdatalag.

Källförteckning

1. Datainspektionen Dnr 998-2007 Beslut [mot Försäkringskassan] efter tillsyn enligt personuppgiftsiagen (1998:204). http://www.datainspektionen.se/Documents/beslut/2007-12-20-forsakringskassan.pdf
2. Datainspektionen, Dnr 1546-2016 om tillsyn enligt personuppgiftslagen (1998:204) – behörighetstilldelning, spärrar m.m enligt patientdatalagen riktad mot Hälso- och sjukvårdsnämnden i Region Gävlebord. http://www.datainspektionen.se/Documents/beslut/2017-04-25-region-gavleborg.pdf
3. Dataskydd.ne, kommentarer till riksdagen om Prop. 2014/15:148 om en ny domstolsdatalag. Skickat till Justitieutskottet. https://dataskydd.net/sites/default/files/domstolsdatalagen_kommentarer_dataskyddnet_ju.pdf
4. Dataskydd.net, remissyttrande över SOU 2015:39 Myndighetsdatalag. https://dataskydd.net/sites/default/files/sou201539_remissyttrande_dataskyddnet.pdf
5. Dataskydd.net, remissyttrande över SOU 2016:65 Ett samlat ansvar för tillsynen av den personliga integriteten. https://dataskydd.net/sites/default/files/sou201665_remissyttrande_dataskyddnet.pdf
6. Dataskydd.net, remissyttrande över SOU 2017:29 Brottsdatalag. https://dataskydd.net/sites/default/files/sou201729_remissyttrande_dataskyddnet_20170711.pdf
7. Deloitte, Deloitte Australian Privacy Index 2015: Transparency is opportunity. https://www2.deloitte.com/content/dam/Deloitte/au/Documents/risk/deloitte-au-risk-privacy-index-2015-090516.pdf
8. ENISA. 2008. Security Economics and the Internal Market. Författare: Ross Anderson, Rainer Boehme, Richard Clayton, Tyler Moore. https://www.enisa.europa.eu/publications/archive/economics-sec
9. Stefan Laube (University of Münster), Rainer Böhme (University of Innsbruck), The Economics of Mandatory Security Breach Reporting to Authorities, presenterad vid The Workshop on the Economics of Information Security, 22-23 juni 2015 i Delft, Nederländerna. http://www.econinfosec.org/archive/weis2015/papers/WEIS_2015_laube.pdf
10. National Conference of State legislatures. Security Breach Notification Laws. [http://perma.cc/7EDG-KVBF]
11. Per Göran Ohlsson, Hans Blackman och Jan Svensson, Ericssons mobiltelefoner 1983–2001, Roos & Tegnér förlag, 2015. Tryckt i Pozkal, Inowrocław, Polen. [finns ej på webben]
12. Regeringen, För ett hållbart digitaliserat Sverige – en digitaliseringsstrategi (N2017/03643/D). http://www.regeringen.se/49adea/contentassets/5429e024be6847fc907b786ab954228f/digitaliseringsstrategin_slutlig_170518-2.pdf
13. SOU 1972:47, Data och integritet. http://weburn.kb.se/metadata/729/SOU_8350729.htm
14. SOU 2008:3, Skyddet för den personliga integriteten - Bedömningar och förslag. http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2008/01/sou-20083/
15. SOU 2015:39, Myndighetsdatalag. http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2015/04/sou-201539/
16. SOU 2016:41, Hur står det till med den personliga integriteten? http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2016/06/sou-201641/
17. SOU 2017:29, Brottsdatalag. http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2017/04/sou-201729/
18. SOU 2017:39, Ny dataskyddslag. http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2017/05/sou-201739/
19. SOU 2017:52, Så stärker vi den personliga integriteten. http://www.regeringen.se/rattsdokument/statens-offentliga-utredningar/2017/06/sou-201752/