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

Dataskydd.net Sverige
c/o Anders Lundquist
Eningebölevägen 44
749 61 Örsundsbro

Justitiedepartementet
103 33 Stockholm

Lund 2015-09-30

Remissyttrande över SOU 2015:73 – Personuppgiftsbehandling på utlännings- och medborgarskapsområdet

Dataskydd.net avstyrker utredningens förslag till ny utlänningsdatalag och ny utlänningsdataförordning. Dataskydd.net lämnar särskilda kommentarer på följande delar av utredningen:

- Kapitel 7.7.5, 7.7.10: om information till den registrerade och till allmänheten.
- Kapitel 7.8: Dataskydd.net avstyrker att den myndighet som utför en behandling eller som det åligger att utföra en behandling ska vara personuppgiftsansvarig för behandlingen.
- Kapitel 7.9: Dataskydd.net avstyrker att insamlade personuppgifter även får behandlas för att tillhandahålla andra [sic] information.
- Kapitel 7.10: Dataskydd.net avstyrker förslagen om utökad korskörning av fingeravtrycks- och fotografiregister.
- Kapitel 7.11: Dataskydd.net avstyrker utredningens förslag om vilka personuppgifter som får behandlas.
- Kapitel 7.12: Dataskydd.net avstyrker utredningens förslag om tillgång till personuppgifter.
- Kapitel 7.13: Dataskydd.net avstyrker utredningens förslag om sökbegränsningar.
- Kapitel 7.14: Dataskydd.net avstyrker utredningens förslag om annat elektroniskt utlämnande än direktåtkomst.
- Kapitel 7.15: Dataskydd.net avstyrker utredningens förslag om direktåtkomst och utlämnande.

Därefter presenterar vi förbättringsförslag inom vart och ett av områdena för var och en av lagarna och förordningarna som utredningen föreslagit ska förändras.

Inledning

Dataskydd.net är kritiska mot att utredningen föreslår en starkt utökad möjlighet till direktåtkomst för myndigheter (särskilt Migrationsverket) i andra myndigheters register. Detta kommer kräva en teknisk anpassning av register på ett sådant sätt att dataskydds- och säkerhetsanpassningar görs svårare.

I utredningskommittén har inte ingått teknisk expertis, eller expertis som företräder individuella dataskyddsrättsliga intressen. Framtida utredningar bör inkludera annan expertis än den juridiska expertis som redan finns representerad. De bör också följa de principer som EU-kommissionen framför om dataminimering, transparens och ansvarsfördelning,[1] samt ge effektiva medel för privatpersoner att skydda sina rättigheter.

Särskilt bör man överväga:

Transparens och insyn

- Bättre användning av samtycke vid utlämning av personuppgifter för att ge individen möjligheter att spåra uppgiftsöverlämningar mellan myndigheter. Se nedan i avsnitten om kapitel 7.11, 7.13 och 7.14.
- Införande av individ-centrisk incident- och sårbarhetsrapportering i syfte att underlätta ansvarsutkrävande för bristande informationssäkerhet. Se nedan i avsnitten om kapitel 7.7.5 och 7.7.10, 7.12 och 7.15.

  Jfr EU-kommissionen (fotnot 1), och PTS (fotnot 5)
- Information till individer som möjliggör granskning – och i förekommande fall reellt ansvarsutkrävande – av att myndigheten agerar i enlighet med sina ändamål och inte samlar in eller behandlar fler personuppgifter än vad som är nödvändigt för dessa ändamål . Se nedan i avsnitten om kapitel 7.7.5 och 7.7.10, 7.8, 7.10.

  Jfr EU-parlamentet (fotnot 25)

Datasäkerhet

- Stadgande av en dataminimeringsprincip, det vill säga att mer uppgifter inte ska samlas in än vad som är absolut nödvändigt för en viss uppgift. Se nedan i avsnitten om kapitel 7.11, 7.12 och 7.13.

  Jfr EU-kommissionen (fotnot 1) och Datainspektionen (fotnot 14)
- Återhållsamhet med direktåtkomst samt bättre planering av varje register och tillhörande applikationer med det i åtanke att tekniska lösningar av dataskydds- och säkerhetsskäl kan behöva uppgraderas och förändras, och att det måste vara någorlunda enkelt att göra. Se nedan i avsnitten om kapitel 7.15.

  Jfr Datatilsynet (fotnot 12)

Bättre ansvarsfördelning

- Inkludera privatpersonerna själva i processen för ansvarsutkrävande (se ovan, rekommendationer för transparens och insyn, samt datasäkerhet).

  Jfr USA (fotnot 3), EU-kommissionen (fotnot 1), EU-parlamentet (fotnot 25)
- Inför bestämmelser om att även personuppgiftsbiträden har direkta skyldigheter gentemot de privatpersoner vars rättigheter ska skyddas. Se nedan i avsnitten om kapitel 7.8, 7.12 och 7.15, samt det avsnitt som behandlar förslagets förhållande till EU-kommissionens förslag till ny uppgiftsförordning från 2012.

  Jfr EU-kommissionen (fotnot 1)

[1] EU-kommissionen COM (2012) 11. Tillgänglig på http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

Kapitel 7.7.5, 7.7.10: om information till den registrerade och till allmänheten

Dagens personuppgiftslagstiftning har rötter i 1970-talet då inställningen till datorer och automatiserad databehandling var att den var alltför komplicerad för privatpersoner att förstå. Vid den tiden var myndigheternas databehandling ett specialiserat område som bara ett fåtal professionella i Sverige begrep sig på. De regler om tillgång till information som finns i både det europeiska direktivet från 1995 och svenska personuppgiftslagen förbiser därför individens intresse av att få reda på tekniska detaljer.

Den tiden är emellertid förbi, och de system som används av myndigheter är inte mer komplicerade att förstå än till exempel appar i smarttelefoner. Det som behövs i dag är mer information till individer, som är anpassad efter vad som krävs för att individer själva ska kunna utkräva ansvar för till exempel bristande säkerhet, behandling i strid med ändamålen eller insamling av onödigt många uppgifter. Myndigheterna har i dag ett onödigt fokus på att ge individer tillgång till uppgifter om sig själva via nätbaserade gränssnitt, oavsett individens egna önskemål. Om uppgifterna är känsliga är det till exempel inte säkert att det av säkerhetsskäl är lämpligt att lägga dem i internetuppkopplade system.[2] Det är inte heller uppenbart på vilket sätt tillgång till den information som myndigheterna har registrerat om personen stärker individens makt och inflytande i förhållande till myndigheten.

Individ-centrisk incident- och sårbarhetsrapportering och ökad användning av samtycke, eller årsrapporter till registrerade om utlämningar av uppgifter från en myndighet kan i stället vara bättre verktyg att öka transparensen till privatpersoner kring datahantering, och dessutom ge privatpersoner ett verktyg att ställa en myndighet till svars om myndigheten inte behandlat uppgifter i enlighet med dataskyddsbestämmelser och/eller misslyckats med att hantera uppgifterna på ett säkert sätt.

I flera amerikanska delstater har man infört obligatorisk incidentrapportering för företag och myndigheter som riktar sig till de privatpersoner som berörs av incidenten. Det finns forskning kring hur konsumenter ställer företag till svars för att inte ha åtgärdat säkerhetsproblem.[3] Någon plikt att rapportera sårbarheter finns inte i USA, men flera större IT-företag har skapat initiativ för så kallade *bug bounties* eller *responsible disclosure*.[4] Målsättningen med dessa är att få säkerhetsproblem kända och åtgärdade så snabbt som möjligt. Åtgärderna är inte

För en mer utförlig behandling av incidentrapportering med vidare forskning och myndighetsrapporter, se Dataskydd.net:s remissyttrande till SOU 2015:23.

[2] Kleja, Monica, Orring, Anna. *Sekretessen hotas av sociala medier*, Ny Teknik, 2013-03-20. http://www.nyteknik.se/nyheter/it_telekom/internet/article3660698.ece

[3] Sasha Romanosky, David Hoffman, Alessandro Acquisti. *Empirical Analysis of Data Breach Litigation* i WEIS 2010; David Solove, ”Are People Really Harmed By a Data Security Breach?”, Concurring Opinions, 22 september 2010; m.fl.

[4] Google Project Zero innebär att ett antal säkerhetsexperter får i uppdrag att leta efter buggar och säkerhetshål i mjukvaror som dels tillhör Google själva, men också sådana buggar och säkerhetshål som kan upptäckas i andra företags mjukvaror. http://googleprojectzero.blogspot.se/; Pwnie Awards är en årlig tävling för den som avslöjat ett särskilt värdefullt och signifikant säkerhetsproblem i någon kommersiell eller offentlig IT-lösning. http://pwnies.com/about/; Pwn2Own är en årlig tävling som syftar till att ge säkerhetsforskare möjligheter att avslöja och uppdagar säkerhetsfel så att dessa kan åtgärdas. https://cansecwest.com/post/2015-03-08-14:42:30_PWN2OWN_2015; Jfr emellertid också öppna diskussioner om nya säkerhetsbrister på branschkonferenser så som Defcon eller Black Hat, eller den europeiska konferensen Chaos Communication Congress, m. fl.; Ett väl utrett och undersökt område är också så kallade *bug bounty awards*. Man kan hitta en sammanställning av befintliga *bug bounty awards* på den här webbsidan: https://bugcrowd.com/list-of-bug-bounty-programs

identiska med, men verkar likna den sårbarhetsrapportering som Post- och telestyrelsen föreslog redan 2006.[5] Det finns enligt Dataskydd.net anledning att tro att ett system som fungerat väldigt bra för att höja IT-säkerhet hos amerikanska apptillverkare också skulle fungera bra för att höja IT-säkerheten i svenska myndigheters appar. Transparens och offentlighet överensstämmer också väl med de principer på vilka svenska myndigheter vill grunda sitt arbete.

Kapitel 7.8: Dataskydd.net avstyrker att den myndighet som utför en behandling eller som det åligger att utföra en behandling ska vara personuppgiftsansvarig för behandlingen

Personuppgiftsansvaret är en av många delar i den svenska dataskyddsrätten där den juridiska föreställningen inte motsvarar en teknisk verklighet. Uppdelningen av ansvar mellan personuppgiftsansvariga och personuppgiftsbiträden är förlegad,[6,7] och inför EU:s dataskyddsreform riktades kritik mot uppdelningen.[8] Den politiska avvägningen blev i slutändan att uppdelningen skulle kvarstå, men med större skyldigheter för personuppgiftsbiträden att säkerställa sig om att personuppgiftsansvarig ställer sådana krav att personuppgiftsansvarig kan uppfylla sina förpliktelser, och en separat möjlighet att söka skadestånd och döma ut viten mot personuppgiftsbiträden. Detta är en utveckling som bör plockas upp i svensk lagstiftning.

KOM(2012)11, Artikel 26(2)(f).

KOM(2012)11, Artikel 75, 77.

Personuppgiftslagen följer dataskyddsdirektivet 95/46/EG från 1995, där personuppgiftsbiträden inte har någon skyldighet att vidta sådana åtgärder som hjälper personuppgiftsansvar att skydda privatpersoners rättigheter. Det är olyckligt att varken den föreslagna domstolsdatalagen eller innevarande utredning om personuppgiftshantering på utlännings- och medborgarskapsområdet inte åtgärdar den av tekniska skäl okloka ansvarsfördelningen.

Prop 2014/15:148 Ny domstolsdatalag

Utredaren observerar till exempel om fingeravtrycksregister att ”i praktiken är det alltså Polismyndigheten som handhar, förvaltar och underhåller [Migrationsverkets fingeravtrycksregister] genom en överenskommelse mellan Migrationsverket och Polismyndigheten. [Migrationsv]erket har alltså ingen möjlighet att registrera, radera eller komma åt uppgifter i sitt eget fingeravtrycksregister utan Polismyndighetens biträde.” Datainspektionen har redan i ett remissvar på departementspromemorian om en ny domstolsdatalag[9] kommenterat på att ansvar måste fördelas mellan myndigheter på ett sådant sätt att den ansvariga myndigheten har realistiska möjligheter att säkerställa dataskyddet.

SOU 2015:73, s. 278

Jämför Dataskydd.net:s kommentarer nedan på kapitel 7.15 om direktåtkomst.

[5] Post- och telestyrelsen. *Strategi för ett säkrare Internet i Sverige*. PTS-ER-2006:12

[6] Traung, Peter. *The Proposed New EU General Data Protection Regulation*, Computer Law Review International. Volume 13, Issue 2, Pages 33–49, september 2013

[7] Artikel 29-gruppen. Opinion 3/2010 on the principle of accountability, juli 2010, p. 46. Tillgänglig på: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf

[8] EU-kommissionen, DG Justice, enhet C.3: dataskydd. *Summary of replies to the public consultation about the future legal framework for protecting personal data*. November 2010. Tillgänglig på http://ec.europa.eu/justice/news/consulting_public/0003/summary_replies_en.pdf

[9] Datainspektionen: Departementspromemorian Domstolsdatalag (Ds 2013:10). Remissyttrande dnr 361-2013. Tillgänglig på: http://www.datainspektionen.se/Documents/remissvar/2013-05-31-domstolsdatalag.pdf

Kapitel 7.9: Dataskydd.net avstyrker att insamlade personuppgifter även får behandlas för att tillhandahålla andra [sic] information

Dataskydd.net observerar att syftet med ändamålsbegränsningen i lagstiftningen är att individen ska ges tillräckliga förutsättningar att förstå hur, och i vilken utsträckning, hen påverkas av andra. Denna rätt att förstå och utöva inflytande över sin egen situation skyddar individens rätt till privatliv och rätt till den egna identiteten. Utredningen har inte haft detta perspektiv i fokus för sin behandling av ändamålsbegränsningen, vilket den borde ha haft.

I den utsträckning man vill tillåta primära och sekundära ändamål med uppgiftsbehandling, där en eller flera av målsättningarna är implicita och där nya målsättningar kan tillkomma allt eftersom myndigheten utvecklar sin verksamhet, behöver man också införa metoder för individer att sätta stopp, överklaga och invända mot sekundära och nytillkomna ändamål.

Kapitel 7.10: Dataskydd.net avstyrker förslagen om utökad korskörning av fingeravtrycks- och fotografiregister

Det är utifrån utredningens beskrivning svårt att föreställa vilka situationer som kan uppstå där automatiska system för bildigenkänning höjer rättssäkerheten och stärker den enskildes integritet. Utvecklingen i omvärlden talar också emot att den sortens automatiska bildbehandlingssystem som utredningen vill möjliggöra verkligen stärker individens integritetsskydd.[10]

Kapitel 7.11: Dataskydd.net avstyrker utredningens förslag om vilka personuppgifter som får behandlas

Utredningens bärande hypotes är att ”[e]tt effektivt utnyttjande av den moderna informationstekniken kan leda till effektivitetsvinster och kostnadsbesparingar för myndigheterna.” Det bör nämnas att de statliga myndigheternas resurser – mätt i årsarbetskrafter – har ökat relativt kraftigt mellan åren 2000 och 2014, inte minskat.[11] Det ökade informationsutbytet mellan myndigheter och mer avancerad e-förvaltning har inte lett till någon påvisbar effektivisering eller kostnadsbesparing.

SOU 2015:73, s. 185

Om många tjänstemän är beroende av en viss applikation för sina vardagliga sysslor blir applikationen emellertid också svår att ändra. Om ett tekniskt system visar sig vara osäkert eller dåligt anpassat för att skydda individers integritet kan det av organisatoriska skäl ändå vara svårt att ändra på och uppgradera. Detta kan i själva verket innebära sämre effektivitet, dålig säkerhet och svagt skydd av individuella rättigheter.

Danska Datatilsynet fann till exempel följande vid en granskning av stora dataintrång på danska myndigheter 2013:[12]

> [a]t hackerangrebet førte til, at bl.a. oplysninger i Schengen-informations-

Datatilsynet, 2013-632-0050

[10] The Register, *Australia to capture biometrics at the border under new law*, 19 augusti 2015. http://www.theregister.co.uk/2015/08/19/australia_to_capture_biometrics_at_the_border_under_new_law/

[11] Förändringar i svensk statsförvaltning och framtida utmaningar, Statskontoret, 2015. s. 59

[12] Datatilsynet (Danmark). 31 juli 2015. Journalnummer 2013-632-0050. *Uvedkommendes adgang til personoplysninger i systemer, som Rigspolitiet er dataansvarlig for* http://www.datatilsynet.dk/afgoerelser/seneste-afgoerelser/artikel/vedroerende-uvedkommendes-adgang-til-personoplysninger-rigspolitiets-jnr-2013-079-76/

> systemet er blevet overført til hackerens computer i Cambodia, må overvejende tilskrives /.../ for omfattende deling af IT-systemmæssige ressourcer som LPAR, operativsystem, diske og RACF mellem de forskellige dataansvarlige[.]

I flera stora utredningar 2015 har regeringen påtalats att den ökade användningen av elektroniska system i flera viktiga basinfrastrukturer skapar nya säkerhetsutmaningar.[13] IT-lösningar med tillhörande säkerhetsproblem på till exempel myndigheter utmålas som ett allvarligt och kritiskt hot mot nationens intressen och säkerhet. Integritetsutredningens förberedelser av nya specialregisterlagar är en viktig del av att skapa system som rimligen kan hållas säkra, både för individer och för myndigheterna själva. Det är viktigt att Justitiedepartementets utredningar om specialregisterlagar inte slätar över dataskyddsfrågor och datasäkerhetsfrågor. Detta identifierades också i utredningsuppdraget där det uttryckligen står ”se till att den reglering som föreslås ger möjlighet att utveckla moderna och ändamålsenliga it-system.”

Se t.ex. SOU 2015:25, s. 226–228

Kommittédirektiv 2014:76, s. 6

Det finns anledning att ställa individens intresse av ett starkt skydd för de mänskliga rättigheterna i fokus för utformningen av myndigheternas informationshantering, i stället för att ihärda med naiva förhoppningar om effektivisering.

I januari 2012 föreslog EU-kommissionen en dataminimeringsprincip i den nya uppgiftsförordningen, som kodifierades och stärktes av Europaparlamentet i september 2013. Dataminimeringsprincipen innebär att man begränsar insamling, behandling och tillgång till personuppgifter till det absoluta minimum som krävs för att ett visst ändamål ska uppnås. Principen har också stöd hos Datainspektionen[14] och amerikanska nationella institutet för teknisk standardisering (NIST).[15] Utredningen har emellertid begränsat sin tillämpning av principen till enskilda tjänstemäns tillgång till uppgifter vid utförandet av specifika sysslor.

KOM(2012)11, Artikel 5(c)

Europaparlamentet, A7-0402/2013

Dataminimeringsprincipen har stora fördelar ur dataskydds- och datasäkerhetssynpunkt.[16] Det är svårare för myndigheterna att kränka individers integritet och privata sfär om uppgiftsinsamlingen är begränsad till det absoluta minimum som krävs för att man ska kunna utföra sina sysslor. Det är också omöjligt att medelst olyckor, säkerhetsfel, slarv eller antagonistiska IT-attacker förlora data man inte samlat in. Både individen och myndigheten blir på det sättet säkrare.

För behandling av känsliga personuppgifter är samtyckesprincipen, en annan grundpelare i den europeiska dataskyddslagstiftningen, av intresse. Utredningen föreslår att individer inte ska ha någon allmän rätt att motsätta sig behandling av personuppgifter, men många av de specifika detaljregler utredningen föreslår skulle enklare och transparentare lösas med samtycke än genom strikt särreglering av uppgiftskategorier i lag. Detta gäller till exempel registrering av asylsökandes sexualitet i syfte att bedöma hotbilden mot den asylsökande i hem-

KOM(2012)11, Artikel 7

Jfr SOU 2015:73, s. 293

[13] SOU 2015:23 – *Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten* samt SOU 2015:25 – *En ny säkerhetsskyddslag*.

[14] Datainspektionen: Inbyggd integritet. Tillgänglig på http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/inbyggd-integritet-privacy-by-design/

[15] National Institute of Standards and Technology. Special Publication 800-122. ”*Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* Tillgänglig på http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

[16] Se bl. a. National Institute of Standards and Technology (NIST). Special Publication 800-122. ”*Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* Tillgänglig på: http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

landet. Om diskussionen kring sexualitet uppstår under asylhanteringen finns goda möjligheter att i stället fråga ifall den asylsökanden också vill inkluderas i ett sökbart register (för statistiska, historiska eller akademiska syften).

Utredningen föreslår att ”känsliga personuppgifter bör få användas som sökbegrepp när det gäller personuppgifter för ändamålen tillsyn, kontroll, uppföljning och planering, framställning av statistik samt testverksamhet.” Det kan inte anses att individens rätt till dataskydd och makt över den egna personligheten stärks av att staten detaljreglerar myndighetens uppgiftsinsamling på ett sätt som individen inte själv kan granska eller motsätta sig. SOU 2015:73, s. 300

Utredningen föreslår i vilket fall att ”en bestämmelse om gallring [bör] införas för personuppgifter som har behandlats för ändamålen tillsyn, kontroll, uppföljning, planering av verksamheten, framställning av statistik eller testverksamhet. Sådana personuppgifter ska gallras direkt när behandlingen inte längre är nödvändig för något av de angivna ändamålen.” Om gallring redan specifikt omnämns som önskvärt, kan det inte vara för begränsande eller förhindrande att istället göra själva insamlingen av uppgiften avhängigt föregående samtycke. SOU 2015:73, s. 326-227

Kapitel 7.12: Dataskydd.net avstyrker utredningens förslag om tillgång till personuppgifter

I utredningen beskrivs att ”handläggare, beslutsfattare och assistenter som har behörighet bara [får] tillgång till de delar av systemet, s.k. applikationer, som de behöver för att kunna fullgöra sina arbetsuppgifter”. Det innebär att de fortfarande får fler uppgifter om en individ än de behöver för att fullgöra sina arbetsuppgifter. I utlänningsdatalagen och domstolsdatalagen föreslås att behörigheten ska avgränsas ännu mer, så att varje tjänsteman bara tar del av precis de uppgifter denne behöver för att genomföra sitt arbete. SOU 2015:73, s. 168 Prop 2014/15:148

Däremot saknas en begränsning av insamlingen av uppgifter. Det är fel att konstruera ett datorsystem utifrån tanken att bara användarna (tjänstemännen på myndigheterna) kan vara dumma mot de registrerade (i detta fall individer som rör sig över gränsen). IT-systemet och registret kan som sådant påverka människor, och vilket fokus man har i konstruktionen av IT-systemet påverkar majoriteten av de registrerade mycket mer och över längre tidsperioder än vad någon enskild användare av systemet kan göra.

I januari 2012 föreslog EU-kommissionen en dataminimeringsprincip i den nya uppgiftsförordningen, som kodifierades och stärktes av Europaparlamentet i september 2013. Denna princip har stora fördelar ur dataskydds- och datasäkerhetssynpunkt.[17] Det är svårare för myndigheterna att kränka individers integritet och privata sfär om uppgiftsinsamlingen är begränsad till det absoluta minimum som krävs för att man ska kunna utföra sina sysslor. Det är också omöjligt att medelst olyckor, säkerhetsfel, slarv eller antagonistiska IT-attacker förlora data man inte samlat in. Både individen och myndigheten blir på det sättet säkrare. KOM(2012)11, Artikel 5(c)

Danska Datatilsynet fann vid en granskning av stora dataintrång på danska myndigheter 2013[18]

> [a]t hackerangrebet førte til, at bl.a. oplysninger i Schengen-informationssystemet er blevet overført til hackerens computer i Cambodia, må overvejende Datatilsynet, 2013-632-0050

[17] Se ovan fotnot 16.
[18] Se ovan fotnot 12.

> tilskrives /.../ for omfattende deling af IT-systemmæssige ressourcer som LPAR, operativsystem, diske og RACF mellem de forskellige dataansvarlige[.]

Av detta borde man utläsa att det fortfarande är insamlingen av, och konstruktionen av, stora register – särskilt populationstäckande register som de som myndigheter ofta har – som är viktig ur dataskydds- och säkerhetssynpunkt.

Korsberoende system för tillgång till uppgifter är i sig själva en säkerhetsrisk. Oförutsedda incidenter riskerar att förvärras och nödvändiga tekniska förändringar för att uppnå bättre säkerhet försenas av att alltför många system är beroende av varandra. De tekniska systemens design, som beror på hur man utformat förutsättningarna för myndigheternas verksamhet, är avgörande för hur starkt dataskydd och hur effektiv datasäkerhet man kan förvänta sig.

Kapitel 7.13: Dataskydd.net avstyrker utredningens förslag om sökbegränsningar

Utredningen föreslår detaljerade bestämmelser för ändamål, känsliga uppgifter, tillgång och sökbegrepp, men det finns ingen möjlighet för individer att granska hur myndigheterna följer dessa bestämmelser och det finns ingen möjlighet för individer att utkräva ansvar av myndigheter som misstänkts och/eller visas hantera uppgifterna fel.[19] Förslagen att ”känsliga personuppgifter bör få användas som sökbegrepp när det gäller personuppgifter för ändamålen tillsyn, kontroll, uppföljning och planering, framställning av statistik samt testverksamhet”, och ”en bestämmelse om gallring /.../ för personuppgifter som har behandlats för ändamålen tillsyn, kontroll, uppföljning, planering av verksamheten, framställning av statistik eller testverksamhet. Sådana personuppgifter ska gallras direkt när behandlingen inte längre är nödvändig för något av de angivna ändamålen”, kan med sin detaljrikedom framstå som extra skyddande, men innebär i praktiken att man individen lämnas med väldigt liten makt.

SOU 2015:73, s. 300

SOU 2015:73, s. 326-227

Ändamålen tillsyn, kontroll, uppföljning och planering, framställning av statistik samt testverksamhet är breda och kan omfatta varje tänkbar tidsperiod. Det saknas möjligheter för individer att motsätta sig eller överklaga myndighetens beslut att behandla uppgifterna. En kombination av dataminimerings- och samtyckesprinciperna vore bra i syfte att stärka individens delaktighet i förvaltningen av sig själv.

Testverksamhet bör inte skötas med personuppgifter! Av uppenbara skäl är testverksamhet av en sådan natur att saker oftare går fel, eftersom man testar saker. Då bör man också bara använda sig av sådana uppgifter som man själv – eller ännu hellre de berörda privatpersonerna – inte har någonting emot att man tappar bort eller förstör. Datainspektionen har tidigare uppmärksammat problemen med att använda riktiga personuppgifter i samband med testverksamhet av IT-system vid en granskning av företaget SJ.[20]

Se också Dataskydd.net:s kommentarer ovan på kapitel 7.11 om vilka personuppgifter som får behandlas.

[19] Se också Dataskydd.net:s kommentarer på Prop 2014/15:148 om ny domstolsdatalag, framförda till riksdagen 15 september 2015. Tillgängliga på: https://dataskydd.net/nyheter/2015/09/15/kommentarer-till-riksdagen-om-prop-201415148-om-en-ny-domstolsdatalag

[20] http://www.datainspektionen.se/press/nyheter/2014/fel-av-sj-anvanda-riktiga-personuppgifter-da-it-system-testades/

Kapitel 7.14: Dataskydd.net avstyrker utredningens förslag om annat elektroniskt utlämnande än direktåtkomst

Utredningen skriver att ”[d]et /…/ inte [bör] införas någon särskild regel om utlämnande av personuppgifter i annan elektroniskt form än genom direktåtkomst i den nya lagen.” Dataskydd.net delar bedömningen att omständigheterna kring utlämning inte behöver detaljregleras, men vill också observera att det inte finns något sätt för en enskild att granska myndigheter som ”ansvarar /…/ för att överföringen sker på ett säkert sätt, till exempel att uppgifterna krypteras innan de överförs till mottagaren.” Utlämningar kan ske utan att individen informeras, vilket gör det svårt för individen att avgöra när det kan finnas någon som är ansvarig för att hens uppgifter behandlas säkert. Även om individen är informerad om att det kan finnas någon som är således ansvarig, finns det inga möjligheter för individen ifrågasätta rimligheten i utlämnandet eller de tekniska omständigheterna kring utlämnandet.

SOU 2015:73, s. 303

SOU 2015:73, s. 303

Individens samtycke är en grundpelare i den europeiska dataskyddslagstiftningen. Utredningen föreslår att individer inte ska ha någon allmän rätt att motsätta sig behandling av personuppgifter, men samtycket kan användas för att undvika många av de specifika detaljregler utredningen föreslår. Samtycke kan vid utlämning av personuppgifter skapa översikt för varje individ om vilka som tar reda på saker om dem, och vilka olika myndigheter som har något ansvar för att deras uppgifter behandlas säkert och ändamålsenligt. Detta gör det enklare för individer att utkräva ansvar av de myndigheter som inte hanterar deras uppgifter på ett säkert och respektfullt sätt, men också att förstå hur olika myndigheter samarbetar med varandra.

KOM(2012)11, Artikel 7

Kapitel 7.15: Dataskydd.net avstyrker utredningens förslag om direktåtkomst

Utredningen föreslår utökad direktåtkomst till uppgifter mellan myndigheter utan att individen informeras eller bereds möjlighet att samtycka. Dels har Polismyndigheten, Säkerhetspolisen, utlandsmyndigheterna, Försäkringskassan, Pensionsmyndigheten och Skatteverket redan direktåtkomst till Migrationsverkets register, men Migrationsverket föreslås också beredas tillgång till tidigare nämnda myndigheters register.

SOU 2015:73, s. 308

Utredningen skriver att ”möjligheten till direktåtkomst ökar riskerna för intrång i den personliga integriteten, eftersom det typiskt sett innebär att uppgifter blir tillgängliga för fler personer och att den utlämnande myndighetens möjligheter att kontrollera användningen av uppgifterna minskar.”

SOU 2015:73, s. 304

Man bör sannolikt av tekniska skäl undvika att skapa alltför många korsberoende applikationer och databaser genom alltför vidlyftiga bestämmelser om direktåtkomst. Ökat informationsutbyte mellan myndigheter behöver inte i sig själv innebära en mer effektiv myndighetsutövning. Tvärtom finns indikationer på att de statliga myndigheternas resurser – mätt i årsarbetskrafter – har ökat relativt kraftigt mellan åren 2000 och 2014 (alltså samtidigt som e-förvaltning blivit mer använt), inte minskat.[21] Varje teknisk applikation för inhämtning och utlämning av personuppgifter som utvecklas på myndigheterna och sprids

[21] Förändringar i svensk statsförvaltning och framtida utmaningar, Statskontoret, 2015. s. 59

mellan dem blir vidare en integrerad del av myndighetens vardagliga verksamhet. Enligt utredningen om en ny myndighetsdatalag är dataregister ”centrala för [myndigheternas] verksamhet [och] viktig[a] medel för att genomföra besparingar och effektiviseringar i förvaltningen”. Utredningens bärande hypotes är att ”[e]tt effektivt utnyttjande av den moderna informationstekniken kan leda till effektivitetsvinster och kostnadsbesparingar för myndigheterna.”

SOU 2015:39, s. 55

SOU 2015:73, s. 185

Det ökade informationsutbytet mellan myndigheter och mer avancerad e-förvaltning har inte lett till någon påvisbar effektivisering eller kostnadsbesparing. Om många tjänstemän är beroende av en viss applikation för sina vardagliga sysslor blir applikationen emellertid också svår att ändra. Om ett tekniskt system visar sig vara osäkert eller dåligt anpassat för att skydda individers integritet, kan det av organisatoriska skäl ändå vara svårt att ändra på och uppgradera. Detta kan i själva verket innebära sämre effektivitet, dålig säkerhet och svagt skydd av individuella rättigheter.

Danska Datatilsynet fann till exempel vid en granskning av stora dataintrång på danska myndigheter 2013[22]

> [a]t hackerangrebet førte til, at bl.a. oplysninger i Schengen-informationssystemet er blevet overført til hackerens computer i Cambodia, må overvejende tilskrives /.../ for omfattende deling af IT-systemmæssige ressourcer som LPAR, operativsystem, diske og RACF mellem de forskellige dataansvarlige[.]

Datatilsynet, 2013-632-0050

I flera stora utredningar 2015 har regeringen påtalats att den ökade användningen av elektroniska system i flera viktiga basinfrastrukturer skapar nya säkerhetsutmaningar.[23] IT-lösningar med tillhörande säkerhetsproblem i till exempel på myndigheter utmålas som ett allvarligt och kritiskt hot mot nationens intressen och säkerhet. Integritetsutredningens förberedelser av ny specialregisterlagar är en viktig del av att skapa system som rimligen kan hållas säkra, både för individer och för myndigheterna själva. Det är viktigt att Justitiedepartementets utredningar om specialregisterlagar inte slätar över dataskyddsfrågor och datasäkerhetsfrågor. Detta identifierades också i utredningsuppdraget där det uttryckligen står ”se till att den reglering som föreslås ger möjlighet att utveckla moderna och ändamålsenliga it-system.”

Se t.ex. SOU 2015:25, s. 226–228

Kommittédirektiv 2014:76, s. 6

Det finns anledning att ställa individens intresse av ett starkt skydd för de mänskliga rättigheterna i fokus för utformningen av myndigheternas informationshantering, istället för att ihärda med naiva förhoppningar om effektivisering.

Direktåtkomsten skapar sämre översikt för varje individ om vilka som tar reda på saker om dem, och vilka olika myndigheter som har något ansvar för att deras uppgifter behandlas säkert och ändamålsenligt.

Korsberoende system för utlämnande av uppgifter och direktåtkomst av uppgifter är i sig själva en säkerhetsrisk. Oförutsedda incidenter riskerar att förvärras och nödvändiga tekniska förändringar för att uppnå bättre säkerhet försenas av att alltför många system är beroende av varandra. De tekniska systemens design, som i sin tur beror på hur man utformat förutsättningarna för myndigheternas verksamhet, är avgörande för hur starkt dataskydd och hur

[22] Se ovan fotnot 12.

[23] SOU 2015:23 – *Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten* samt SOU 2015:25 – *En ny säkerhetsskyddslag*.

effektiv datasäkerhet man kan förvänta sig.[24]

Förhållandet till EU-kommissionens dataskyddsförslag och förslag

Utredningen har mot bakgrund av EU:s pågående dataskyddsreform fått i uppdrag att ”i sitt arbete noga följa den fortsatta behandlingen inom EU av förslaget till ny dataskyddsreglering samt anpassa de förslag till författningsreglering som lämnas till denna översyn och dess resultat.” EU:s pågående dataskyddsreform är utformad kring ett antal enkla principer som inte har införlivats, eller bara delvis införlivats, i utredningens förslag. I enlighet med den benämning av de grundläggande principerna som togs fram av Europaparlamentet i september 2013[25] anser Dataskydd.net att det fortfarande finns anledning att arbeta med:

Kommittédirektiv 2014:76, s. 5

- Laglighet, korrekthet och öppenhet. (Europaparlamentet, A7-0402/2013, Artikel 5(a)).
- Dataminimering. (Europaparlamentet, A7-0402/2013, Artikel 5(c)).
- Effektivitet. (Europaparlamentet, A7-0402/2013, Artikel 5(ea)).

Med effektivitet har Europaparlamentet avsett individens möjligheter att säkerställa sig om att hens rättigheter faktiskt respekteras. För detta krävs öppenhet och transparens kring behandlingen, som i dag inte återfinns i svensk rätt. För specifika förslag, se inledningen.

Dataminimering är en viktig princip, men också en vettig säkerhetsåtgärd. En tydlig ändamålsbegränsning borde vara tillräcklig för att privatpersoner och myndigheter ska kunna avgöra vilken typ av uppgifter som samlas in.

Svensk dataskyddslagstiftning är i behov av en uppdaterad syn på ansvarsfördelningen mellan personuppgiftsansvariga och personuppgiftsbiträden, motsvarande den som EU-kommissionen förslagit i den nya dataskyddsförordningen.

KOM(2012)11, Artikel 26
KOM(2012)11, Artikel 77
m.m.

Som i EU-kommissionens förslag till dataskyddsförordning bör man införa en uttrycklig möjlighet för organisationer att representera enskilda eller grupper av enskilda i klagomål mot myndigheter. Dessutom behövs, precis som i EU-kommissionens förslag till dataskyddsförordning, effektiva sanktioner mot aktörer som bedömts agera fel.

KOM(2012)11, Artikel 73(2)

KOM(2012)11, Artikel 77-78

Amelia Andersdotter
Ordförande, Dataskydd.net

[24] Anderson, Ross. *Managing the Development of Secure Systems* ur Security Engineering, second version. Tillgänglig på: http://www.cl.cam.ac.uk/~rja14/Papers/SEv2-c25.pdf

[25] Europaparlamentets lagstiftningsresolution av den 12 mars 2014 om förslaget till Europaparlamentets och rådets förordning om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (allmän uppgiftsskyddsförordning) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)). A7-0402/2013. Tillgänglig på: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//SV