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

Dataskydd.net Sverige
Alsnögatan 18
116 41 Stockholm

Justitiedepartementet
103 33 Stockholm

Uppsala 2018-01-23

Remissyttrande över EU:s dataskyddsreform – anpassningar av vissa författningar om allmän ordning och säkerhet – Ds 2017:58 (dnr Ju2017/09003/L4)

Innehållsförteckning:

Sammanfattning

Promemorian förhåller sig inte till den europeiska dataskyddslagstiftningen så mycket som den arbetar sig runt den. Eftersom målsättningen förefaller vara att slippa förändra saker i svensk rätt, snarare än att tillgodose efterlevnaden av det europeiska regelverket eller stärka privatpersoners dataskydd, är resultatet inte tillfredsställande. Utredaren överhänvisar till *allmänt intresse* (en sorts catch-all som många dataskyddspromemorior hänvisat till när de inte vill hitta någon annan rättslig grund) och har inte tittat närmare på den distinktion mellan rättslig grund och ändamål som är tydlig i europeisk rätt, och vag i svensk. Dataskydd.net är kritiska mot att regeringskansliet hanterar den största översynen av svenska registerförfattningar sedan sent 1990-tal på detta sätt.

Det allmänna intresset

I vårt remissyttrande över SOU 2017:39 Ny dataskyddslag framhöll vi att myndigheters verksamhet inte per definition kan vara ett allmänt intresse.[1] I denna promemoria görs ytterligare påståenden om allmänna intressen.

Ett allmänt intresse eller ett allmänintresse kan så klart i teorin definieras hur som helst. Skälen i dataskyddsförordningen ger ingen särskild ledtråd om vad en absolut gräns för det allmänna intresset skulle vara, även om många skäl exemplifierar allmänna intressen med folkhälsa.[2] Det behöver inte vara ett uttryck för vad som egentligen är ett allmänt intresse, utan kan vara ett uttryck för vilka intressegrupper som varit mest aktiva i påverkansarbetet när dataskyddsförordningen fortfarande var föremål för politiska förhandlingar.

I Niklas Dahls examensarbete *Tillvaratagandet av allmänna intressen*, skrivet vid Juridiska fakulteten i Lund vårterminen 2014,[3] framhåller Dahl att allmänintresset är vad helst politikerna bestämmer att det ska vara.[4] Det behöver inte gynna en bredare grupp människor, utan kan också vara till gagn för bara ett fåtal, och allmänintresset kan också bestämmas utifrån ekonomiska faktorer.[5] Till exempel kan politiker bestämma att en viss sektor (eller ett visst företag) är så viktig(t) att det ligger i allmänintresset att subventionera eller på annat sätt stödja sektorn eller företaget.

Promemorian förefaller ha ägnat sig åt någonting liknande det senare, när det hävdar att kreditupplysning och inkassoverksamhet är av allmänt intresse för att enskilda intressenter på marknaden genom sådana institutioner får förenklade transaktioner.[6] Synsättet finner emellertid inte stöd i dataskyddsförordningen.

I den engelska språkversionen av dataskyddsförordningen används begreppet *public interest* som betyder ”*the welfare or well-being of the general public; commonwealth*” eller ”*appeal or relevance to the general populace.*”[7] I den rumänska språkversionen används begreppet *interest public*, som återigen betyder ”*care privește pe un popor întreg: interest public*” [översättning: som angår/härrör till

[1] Dataskydd.net:s remissyttrande över SOU 2017:39 Ny dataskyddslag.
[2] Dataskyddsförordningen skäl 54, skäl 159.
[3] Dahl, Niklas, Tillvaratagandet av allmänna intressen, examensarbete på juristprogrammet, Lunds universitet, VT 2014.
[4] Ibid., s. 21.
[5] Ibid., s. 17.
[6] Ds 2017:26, s. 39.
[7] Random House Dictionary, 2017.

en hel befolkning].[8] Det finns alltså skäl att tro att dataskyddsförordningens *allmänintresse* inte är det formbara *allmänna intresse* som finns i svensk rätt.

Ändamål och rättslig grund är inte samma sak

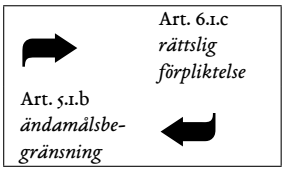
Som redan påtalats av utredningen om en ny brottsdatalag har det skett en sammanblandning mellan vad som i dataskyddsrättslig mening är särskilt bestämda ändamål och tillåtna rättsliga grunder för behandling.[9]

Bedömningen som görs i promemorian är sannolikt färgad av att utredaren betraktar fastställandet av ändamål och fastställandet av rättslig grund för behandling som i princip samma sak, vilket det inte är. Ett ändamål kan (och ska)[10] fastställas *av den personuppgiftsansvarige* givet att denna får en *rättslig förpliktelse* eller har någon annan rättslig grund för sin behandling. För myndigheter inom området för allmän säkerhet och ordning borde det typiskt sett vara rättsliga förpliktelser som är den rättsliga grunden, eftersom myndigheters verksamheter ska ha stöd i lag. Vårt synsätt reflekteras i dataskyddsförordningens skäl 50:

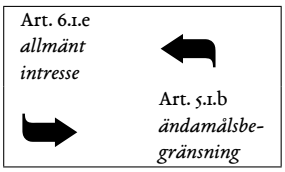
> Den rättsliga grund för behandling av personuppgifter som återfinns i unionsrätten eller i medlemsstaternas nationella rätt kan också utgöra en rättslig grund för ytterligare behandling. För att fastställa om ett ändamål med den ytterligare behandlingen är förenligt med det ändamål för vilket personuppgifterna 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.
>
> – Dataskyddsförordningen, (delar av) skäl 50.

Men invändningarna mot att sammanblanda ändamål och rättslig grund är inte bara teoretiskt tillfredsställande utan har en praktisk karaktär för enskilda (registrerade). Om den personuppgiftsansvarige har en skyldighet att ta ställning till och dokumentera sitt efterlevande av principerna i dataskyddsförordningen artikel 5, givet deras skyldigheter och uppdrag, är det större sannolikhet att den enskilde kan få tag på information enligt artiklarna 13, 14 och 22 som låter denne utöva sina rättigheter effektivt. Istället för att behöva utveckla en god

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.

[8] https://dexonline.ro/definitie/public def. Șăineanu, ed. VI (1929).

[9] 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 Informationshanteringsutredningens 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.

[10] Se dataskyddsförordningen art. 5.2 (ansvarsskyldighet).

kännedom om systemet för registerförfattningar, kan den enskilde förlita sig på de rättigheter hen har enligt dataskyddsförordningen och EU:s stadga.

EU-förordningar, EU-domstolen och stadgan

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 enskilda 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.

Den innevarande promemorian, precis som alla andra tusentals sidor av statliga utredningar som skrivits det senaste året, har inte behandlat denna omständighet på något sätt alls. Det är ett misstag, eftersom konflikterna kring bland annat datalagring till följd av Tele2-målet och Digital Rights Ireland-målet visat att spänningarna som följer av EU-domstolens avgöranden kan bli mycket svåra att hantera.

Särregleringar av enstaka databaser

Registerförfattningarna har uppstått under en tid då automatiserad databehandling (ADB) i princip var förbehållen stater och andra större institutioner som kunde köpa stordatorer och processorkraft. Idag är detta inte fallet och de flesta tjänstemän äger idag mobiltelefoner med högre beräkningskapacitet än de maskiner registerförfattningarna är skrivna för. Det gör att skyddet för den personliga integriteten inte blir starkare av att man har en särskild lag för varje register som reglerar hur datorn som innehåller registret ska programmeras, men däremot blir flexibiliteten i förvaltningen lägre.

Integritetskommittén har observerat att de stora problemen inom e-förvaltningen snarare är hur nyare tjänster för moderna maskiner utvecklas.[11] Medarbetarnas egna tjänstedatorer är tillräckligt för att kränka den personliga integriteten, till exempel genom profilering. De har föreslagit att fenomenet ska utredas vidare.[12]

Ett genomtänkt skydd för den personliga integriteten behöver idag förhålla sig till många fler datorsystem och många fler aktörer än vad som var fallet på 1970- och 80-talen. Men registerförfattningarna skulle behöva genomlysas med avseende på vilka av deras bestämmelser som faktiskt bidrar till ett starkare integritetsskydd och vilka som inte gör det. Vi ger några exempel:

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.[13] Kontrollåtgärder som riktas mot individer, som individer inte har någon möjlighet att värja sig emot eftersom deras

[11] SOU 2016:41, s. kap. 11.1.
[12] SOU 2017:52, kap. 8.2.3.
[13] Jfr RiR 2010:18.

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 kränkningar av den personliga integriteten inte uppstår. 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 personlig 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 enskildas skydd för den personliga integriteten. 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*).[14] Sökbegränsningarna motiveras i vissa fall sekundärt med att det krävs

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

specifika begränsningar av offentlighetsprincipen enligt tryckfrihetsförordningen,[15] 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, i stället för att ge paragraferna funktionen av specifikation för användargränssnitt.

Om lagar

Kustbevakningsdatalag

Dataskydd.net är inte positiv till speciallagstiftning för myndigheter, och den föreslagna lagtexten exemplifierar i hög utsträckning varför.

Den föreslagna 12 § 3 st gör till exempel att 12 § 1 st i princip aldrig kommer att tillämpas. Om känsliga uppgifter inte ska behandlas (12 § 1 st) annat än i ärendehanteringen (8 §, hänvisad via 12 § 3 st) eller när det finns särskilda skäl (12 § 2 st), så betyder ju det egentligen att känsliga personuppgifter alltid kan behandlas. I alla fall så länge utredaren föreställer sig att myndigheterna inte okynnesbehandlar uppgifter bara för att få behandla lite uppgifter.

Undantaget är huvudregeln.

När man tillämpat alla undantagen från den presumtiva huvudregeln i 12 § 1 st återstår ingenting av förbudet mot behandling av känsliga personuppgifter.

Om tanken är att Kustbevakningen alltid ska få behandla känsliga personuppgifter när den får behandla personuppgifter, är det bättre att inte införa en bestämmelse som ger intryck av att det skulle vara på något annat sätt. Den nuvarande formuleringen är oärlig, och gör också lagstiftningen svår att förstå.

Ändamålsbestämmelserna i 7–11 §§ är onödiga, av anledningar vi ovan anfört. Vi är också kritiska mot bestämmelser om sökbegränsningar (13 §), eftersom denna sorts tekniska funktionalitet borde följa av bestämmelserna om inbyggt integritetsskydd i dataskyddsförordningen art. 25. Genom att skapa lagregler om vissa tekniska funktioner, men inte om andra, kan myndigheterna få intrycket av att inbyggt integritetsskydd bara är viktigt om det först specificerats i lag vad en sådan integritetsskyddande funktion skulle kunna vara. Så är inte fallet. Inbyggt integritetsskydd behöver genomföras tekniskt, inte juridiskt, och det är därför den europeiska bestämmelsen är flexibel och öppen, snarare än specifik och begränsande.

Kustbevakningsdataförordning

Det är inte klart varför Riksarkivet, snarare än Datainspektionen, ska fatta beslut om gallring.[16]

[15] *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.

[16] Jfr Dataskydd.net:s remissyttrande över SOU 2017:39 Ny dataskyddslag.

Vapenlagen

Beskrivningen av hur de *ändamål* som kan göra det *absolut nödvändigt* enligt 1a kap. 3 § att behandla känsliga personuppgifter är otydlig. Som Dataskydd.net anfört vid flera tillfällen innebär den nuvarande lagstiftningstekniken regeringen använder för dataskyddslagar att myndigheterna kan förledas att tro att de inte själva behöver göra ändamålsprövningar eller tillämpa dataskyddsprinciper.

De föreslagna Dataskyddslag och Brottsdatalag innehåller inga bestämmelser att polisen eller någon annan myndighet skulle behöva dokumentera när de upplever något som absolut nödvändigt för något särskilt ändamål, eller alls pröva huruvida ett ändamål är rimligt och lämpligt givet myndighetens uppdrag. Regeringen lovar ju nämligen, genom dataskyddslagen, att regeringen redan gjort denna bedömning.[17]

Det är olyckligt att det inte är tydligare hur man tänker sig att lagstiftningen ska följas upp. Det skapar osäkerhet för medborgare och otydlighet i lagstiftningen. Bestämmelser som den föreslagna i 1a kap. 3 § har säkerligen har goda avsikter, men i praktiken betyder de inget. Falskt skydd och falsk säkerhet kan vara värre än inget skydd alls, och bli regeringen påkommen med att skapa falskt, i stället för reellt, skydd kan det skada medborgarnas förtroende för regeringen.

Falskt skydd är inget skydd.

Det är ingen mening med att ha bestämmelser i lagstiftning som inte går att följa upp eller efterleva. Lagstiftning är ingen utsmyckningsåtgärd, utan bör tas på allvar även av regeringskansliet.

Om man i stället väljer en lagstiftningsmodell där myndigheterna själva formulerar och motiverar behandlingsändamål utifrån sina tydligt, i lag, definierade uppdrag, kan regeringen säkerställa sig om att dokumentation kring vad som funnits vara *absolut nödvändigt* finns tillgänglig. Finns det tillräcklig dokumentation ökar även möjligheterna för både tillsynsmyndigheten och medborgare att säkerställa sig om att lagen faktiskt efterlevs.

För 1a kap. 4 § är invändningarna analoga med invändningarna mot Kustbevakningsdatalag 13 § (se ovan).

Utredaren borde ha föreslagit att 1a kap. 8 § tas bort. Det följer av principen om ändamålsminimering i dataskyddsförordningen art. 5, och av reglerna om rättslig grund i dataskyddsförordningen art. 6, att polisen inte kan använda ett vapenregister hur som helst. Regeringen borde ägna mer tid åt att ge myndigheterna väl definierade uppdrag, utifrån vilka myndigheterna själva kan tillämpa dataskyddets principer på ett väl dokumenterat sätt, i stället för att sitta och mecka med registerändamål.

Lagen om belastningsregister

Utredaren föreslår så vitt vi kan se att förändra uppdragsområdet inom vilket myndigheter med tillgång till registret kan använda uppgifter ur registret. Belastningsregistret ska numera användas för att förebygga, förhindra, upptäcka och utreda brott, i stället för att förebygga, upptäcka och utreda brott. Förändringen motiveras med att uppgifter som lämnats ut ur registret och vidarebehandlas i brottsutredande verksamhet faller under annan lagstiftning än lagen om belastningsregister.[18]

Frågan är om det nya ordet *förhindra* lägger till något användningsområde för uppgifterna som inte redan tidigare täcktes av ordet *förebygga*, eller om

[17] Se även Dataskydd.net:s kommentarer på SOU 2017:39, Ny dataskyddslag.
[18] Ds 2017:58, s. 167.

utredaren bara tyckt att uppräkningen av ord ser snyggare ut om orden är fyra i stället för tre. Någon vägledning finns tyvärr inte i utredningstexten.

Det ser ut som ett subtilt försök att skapa större otydlighet kring vad myndigheter får och inte får göra mot privatpersoner. Luddig lagstiftning hjälper ingen, men minst hjälper det (typiska) medborgare som till skillnad från myndigheter inte har egna heltidsanställda jurister (oftast).

Den föreslagna bestämmelsen i 9 § begränsar privatpersoners rätt till information jämfört med dataskyddsförordningen. Genom en hänvisning till en annan föreslagen bestämmelse i Brottsdatalag (som Dataskydd.net tidigare påtalat fråntar privatpersoner rättigheter som den europeiska lagstiftaren velat ge dem även enligt dataskyddsdirektivet.[19]) minskar man effektivt privatpersoners rättigheter så som etablerade i europeisk och tidigare även svensk rätt. Vi föreslår att regeringen i stället använder rätten till information i dataskyddsförordningen som utgångspunkt för individens rättigheter.

Tre blev fyra.

Det är oklart varför listan över möjliga anledningar att hämta uppgifter ur registret utökas, eftersom två av orden i den nya listan är synonymer och inte uppenbart har helt egna betydelser inom svensk rätt. Om det inte är ett stilistiskt val (vilket det inte borde vara, eftersom lagstiftning ska tas på allvar, vara tydlig och inte i onödan utsmyckas med ovidkommande formuleringar) måste det framgå vad det i stället är för val.

Lagen om misstankeregister

Problemen med dessa förslag är samma som problemen med förslaget till ändringar i lagen om belastningsregister (se ovan).

Lagen om Schengens informationssystem

EU-parlamentet har i EU:s reformarbete i betydligt högre utsträckning än regeringens utredare framhävt dataskyddsförordningen roll i regleringen av Schengens informationssystem.[20]

Dataskydd.net hade velat se en omvärderingar av 9 § 1 st, som utökar SIS II-registret bortom vad som föreskrivs i europeisk rätt. Det hade också varit bra med en robust process för att se efter att registreringen enligt 6 § i lagen om Schengens informationssystem faktiskt efterföljs. Tillsynsmyndigheten, Datainspektionen, har så vitt går att utröna av deras webbplats, aldrig genomfört någon tillsyn av SIS II-systemet, utan förlitar sig i stället på den europeiska koordinerade tillsynen hos Europeiska datatillsynsmannen. Det är otillfredsställande, i den utsträckning Sverige bestämt sig för att ge SIS II ett bredare användningsområde än vad de europeiska lagstiftaren föreställt sig.

Hänvisningen till skadeståndsbestämmelsen i föreslagen brottsdatalag begränsar enskildas rätt till skadestånd i förhållande till skadeståndsbestämmelserna i dataskyddsförordningen art. 82. Utredaren motiverar inte varför man behöver begränsa möjligheten att få skadestånd vid felaktig behandling i förhållande till dataskyddsförordningen, annat än med att det är tillåtet enligt dataskyddsdirektivet att införa skadeståndsbestämmelser vid dataskyddskränkningar.[21]

Förordning om införsel av farliga föremål

Den föreslagna förändringen är obegriplig och motiveras inte närmare. Vapenlagen 1a kap. 7 § reglerar förekomsten av ett vapenregister. Vapenlagen 1a kap. 8 § reglerar vapenregistrets ändamål. Utredaren menar nu att en hänvisning till

[19] Se Dataskydd.net remissyttrande över SOU 2017:29.
[20] EU-parlamentet, A8-0347/2017, A8-0348/2017, A8-0349/2017.
[21] Ds 2017:58, s. 255.

Vapenlagen 1a kap. 8 § behövs i förordningen om införsel av farliga föremål i ”tillämpliga delar”.

Det är oklart på vilket sätt tillämplighet av Vapenlagen 1a kap. 8 § bidrar till detta, och varför ett sådant bidrag inte hittills varit nödvändigt eller skulle ha blivit nödvändigt nu.

En spekulation är att den lagstiftningsteknik med innebörd att regeringen tar över uppdraget med ändamålsbegränsning från myndigheter som i och för sig har väl definierade arbetsuppgifter skapar ogenomtränglig och mystifik lagtext.

Förordning om Schengens informationssystem

Dataskydd.net är oroliga för omöjligheten i att tillse de tillämpliga reglerna. Vem granskar om direktåtkomsten som i förordningen tilldelas tre olika myndigheter faktiskt används på ett ändamålsenligt sätt?

Det är oklart varför förordningen begränsar privatpersoners rättigheter enligt dataskyddsförordningen, som annars är tillämplig lag. Varför ska rättelse ske bara inom tre månader, i stället för “utan dröjsmål”? Vid den sameuropeiska tillsynen av Schengens informationssystem har EDPS observerat att privatpersoner bara i begränsad utsträckning utnyttjar sina rättigheter enligt reglerna om SIS II.[22] Dataskydd.net tror att fler privatpersoner kommer ha bättre möjlighet att utnyttja sina rättigheter, om rättigheterna är lätta att förstå och liknar varandra mellan olika lagstiftningar.

Vi föreslår att medborgare ska informeras en gång per år om vilka registreringsåtgärder som vidtagits mot dem själva av någon brottsbekämpande myndighet.

Förordning om förenklat uppgiftsutbyte mellan brottsbekämpande myndigheter i Europeiska unionen

Ingen kommentar.

Förordning om behandling av personuppgifter i Nationellt forensiskt centrums uppdragsverksamhet

Ingen kommentar.

Förordningen om utdrag ur folkbokföringsdatabasen i och för utredning angående brott m.m.

Förordningen är inte från början väl genomtänkt, eftersom den ger brottsbekämpande myndigheter ett *carte blanche* att utan dokumentation, anledning eller misstanke begära ut uppgifter om enskilda. Utredaren borde ha observerat att detta rimmar illa med det ansvarsutkrävande som den europeiska dataskyddslagstiftningen etablerar.

Bara den omständighet att något varit på ett sätt under lång tid är inte tillräckligt för att det även fortsättningsvis ska vara så. Det är inte heller sant att folkbokföringsdatabasen har som huvudsakligt ändamål att underlätta brottsutredningar, vilket utredaren verkar påstå.[23]

Carte blanche.

Att man år 1967, innan Sveriges första datalag, införde befogenheter för brottsbekämpande myndigheter som inte rimligen överensstämmer med de rättssäkerhetsregler Sverige är förpliktigade att efterleva enligt både Europakonventionen och EU-rätten, är ingen god anledning att strunta i att åtgärda problemet med den dåliga rättssäkerheten när man nu har möjligheten.

[22] EDPS, SIS II Supervision Coordination Group, Report on the exercise of the rights of the data subject in the Schengen Information System (SIS), October 2017.

[23] Ds 2017:58, s. 265.

Källförteckning

1. Dataskydd.net, remissyttrande över SOU 2017:29.
2. Dataskydd.net, remissyttrande över SOU 2017:39.
3. EDPS, SIS II Supervision Coordination Group, Report on the exercise of the rights of the data subject in the Schengen Information System (SIS), October 2017. https://edps.europa.eu/sites/edp/files/publication/14-10-28_report_on_the_exercise_of_the_rights_of_the_data_subject_in_sis_ii_en.pdf
4. Europaparlamentet, A8-0347/2017. http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&mode=XML&reference=A8-2017-0347&language=EN
5. Europaparlamentet, A8-0348/2017. http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&mode=XML&reference=A8-2017-0348&language=EN
6. Europaparlamentet, A8-0349/2017. http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&mode=XML&reference=A8-2017-0349&language=EN