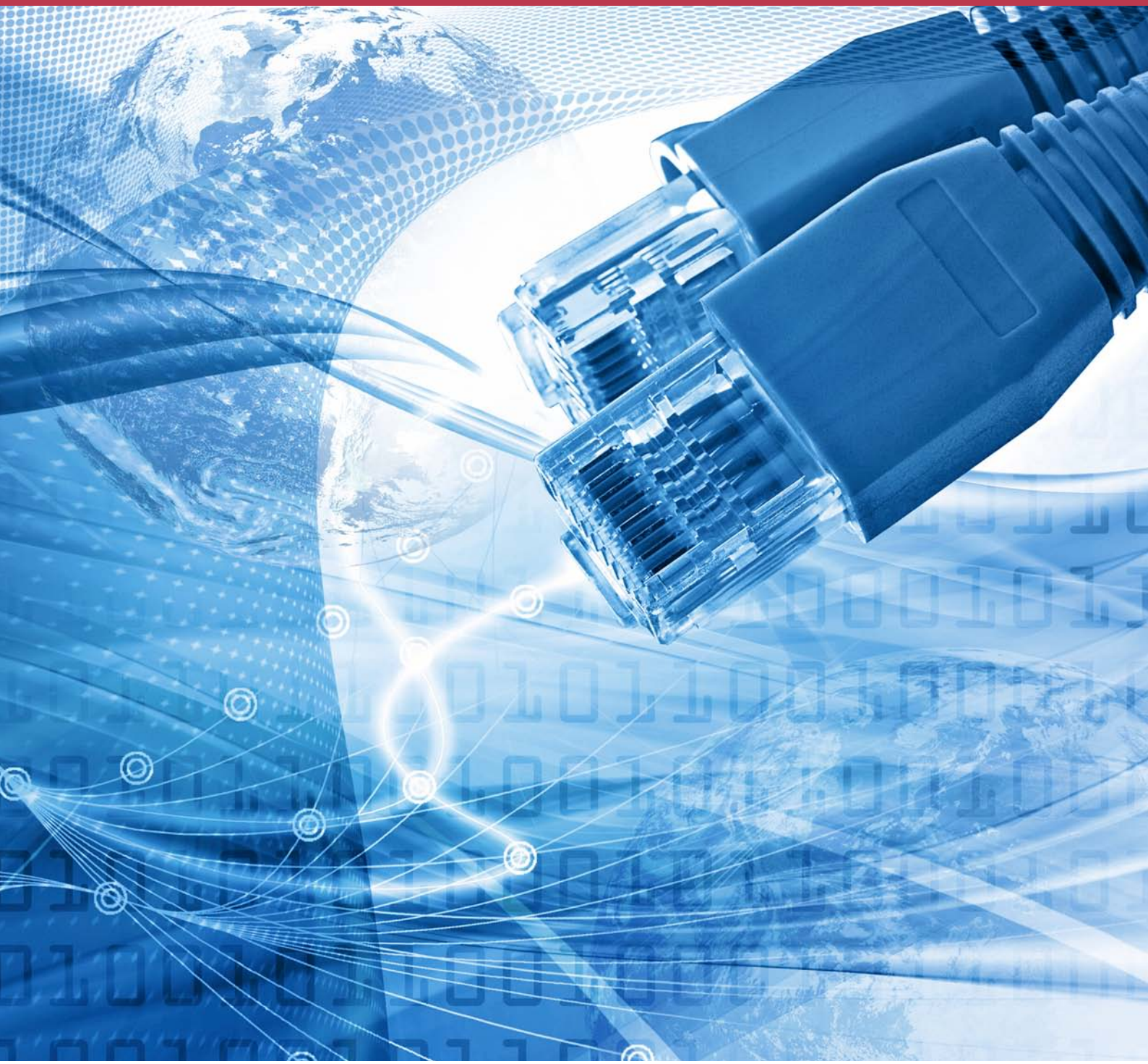

Rättsväsendets informationsförsörjning och den personliga integriteten

Datainspektionens rapport 2012:1

Datainspektionen

Rättsväsendets informationsförsörjning och den personliga integriteten
Datainspektionens rapport 2012:1
Denna rapport finns att ladda ner på www.datainspektionen.se/ladda-ner

Innehåll

Inledning 4
Rättsväsendets informationsförsörjning 5
Datainspektionens tillsyn 6
Regler till skydd för den personliga integriteten 8
Myndigheterna i RIF 7 13
En kortfattad beskrivning av aktuella system 19
Brottmålsprocessen – ett exempel 23
Elektronisk överföring av uppgifter inom rättsväsendet 25
Sekretessbrytande bestämmelser och elektroniskt utlämnande 28
Myndigheternas personuppgiftsansvar 34
Riktiga uppgifter och korrekt behandling 36
Behörighet och spårbarhet 37
Känsliga personuppgifter 44
Bevarande av uppgifter 47
Datainspektionens bedömning 51
Sammanfattning 62

Inledning

Datainspektionen har bedrivit tillsyn gentemot de myndigheter som från regeringen fått ett uppdrag att i brottmålsprocessen skapa ett elektroniskt informationsflöde mellan sig – *rättsväsendets informationsförsörjning (RIF*). I den information som skickas mellan myndigheterna ingår det många personuppgifter och uppgifterna är ofta av integritetskänslig karaktär. Syftet med tillsynsprojektet har varit att granska om, och i så fall hur, bestämmelserna som gäller till skydd för den personliga integriteten följs, när personuppgifter överförs mellan myndigheterna inom RIF.

Det är de myndigheter som nu arbetar aktivt inom RIF som har varit föremål för inspektionen – Rikspolisstyrelsen (RPS), Åklagarmyndigheten (ÅM), Domstolsverket (DV), Kriminalvården (KV), Ekobrottsmyndigheten (EBM), Skatteverket (SKV) och Brottsförebyggande rådet (Brå).

Tillsynen har visat att det inom RIF inte skett någon gemensam analys eller ställningstagande av vilka konsekvenser RIF har för den enskildes personliga integritet och följaktligen inte heller hur skyddet ska upprätthållas eller stärkas. Kunskapen och medvetenheten om reglerna till skydd för den personliga integriteten har också varierat mycket mellan myndigheterna.

När integritetskänsliga uppgifter överförs mellan stora IT-system uppkommer flera viktiga frågor, såsom hur felaktiga personuppgifter ska rättas, hur restriktiviteten vid behandling av känsliga personuppgifter ska kunna upprätthållas, hur åtkomsten till uppgifterna begränsas och följs upp. Denna typ av frågor måste ställas av den enskilde myndigheten, men också i det gemensamma RIF-arbetet. Datainspektionen anser att det i arbetet ska ske en kontinuerlig kartläggning av konsekvenserna för den personliga integriteten. De behov av åtgärder som identifieras vid kartläggningen bör i första hand lösas genom att funktioner skapas i systemen som skyddar den enskildes integritet. Om det inte är möjligt eller lämpligt att skapa skyddet i systemen, bör det istället ske genom överenskommelser mellan myndigheterna och genom införande av rutiner.

En närmare redogörelse för Datainspektions bedömning återfinns i de två sista avsnitten av denna rapport, *Datainspektionens bedömning* och *Sammanfattning*. Tillsammans med avsnittet *Brottmålsprocessen – ett exempel* ger de en överskådlig vy av vad RIF innebär för den personliga integriteten och vad Datainspektionen har för synpunkter. De övriga delarna av rapporten beskriver RIF, Datainspektionens tillsynsprojekt, rättsregler som gäller för behandling av personuppgifter hos myndigheterna inom RIF och myndigheternas egna uppgifter i enkätsvaren.

Rättsväsendets informationsförsörjning

Rättsväsendet har sedan 1996 ett uppdrag att införa ett elektroniskt informationsflöde i brottmålsprocessen. Idag är det elva myndigheter som har regeringens uppdrag att verkställa strategin för samordning av *rättsväsendets informationsförsörjning (RIF*) – Rikspolisstyrelsen, Åklagarmyndigheten, Domstolsverket, Kriminalvården, Ekobrottsmyndigheten, Skatteverket, Brottsförebyggande rådet, Tullverket, Kustbevakningen, Rättsmedicinalverket och Brottsoffermyndigheten.[1]

> *Avsikten med RIF är att skapa en effektivare ärendehantering och förbättra kvaliteten genom att uppgifter som återkommer hos de olika myndigheterna bara ska registreras en gång i ett system och därefter ska de skickas vidare inom rättskedjan till de övriga myndigheternas system när uppgifterna behövs där. Regeringens ambition är också att arbetet ska leda till stärkt medborgarservice och förbättrad möjlighet att analysera brottsligheten och verksamhetsresultaten.*[2]

Arbetet leds sedan våren 2009 av Justitiedepartementet som har bildat en särskild enhet för denna uppgift, *Enheten för samordning, utveckling och informationsförsörjning (SI-enheten).* På myndighetsnivå samordnas RIF av *Rådet för rättsväsendets informationsförsörjning* som består av alla berörda myndigheters generaldirektörer. RIF-rådet beslutar om vad som ska överföras och när i tiden det ska ske. Under RIF-rådet finns det undergrupper som preciserar RIF-rådets beslut och konkretiserar det som är gemensamt för rättskedjan.

Myndigheterna har sina egna system och RIF-arbetet syftar till att länka dessa samman så att uppgifter kan överföras mellan systemen. För närvarande pågår den första etappen som ska skapa ett framåtriktat huvudflöde mellan de myndigheter som ingår i vad som kallas *RIF7* dvs. RPS, ÅM, DV, KV, EBM, SKV och Brå. I denna första etappen ska det även skapas ett nytt system för rapportering av brottmålsavgöranden och det nuvarande systemet *rättsväsendets informationssystem*, det så kallade *RI-systemet*, fasas ut. Genomförandet av den första etappen ska vara klar till halvårsskiftet 2013. Utfasningen av RI-systemet planeras dock bli klart först i januari 2014.[3] Regeringen har den 11 oktober 2012 beslutat om den andra etappen som till att börja med ska löpa parallellt med den första etappen.[4]

1 Regeringsbeslut 1996-11-21 dnr JU96/3163, 050421 Ju2004/11719/PO 021221 dnr JU2006/10392/PO
2 Prop. 2011/12:1 utgiftsområde 4 avsnitt 2.4.1.
3 RIF7-rådets beslut 7 december 2012
4 Regeringsbeslut 2012-10-11 Uppdrag att utveckla rättsväsendets informationsförsörjning Ju2012/6639/SI

Riksrevisionen granskade år 2011 RPS, ÅM, DV, KV och regeringens styrning av arbetet i RIF. Granskningen hade främst ett effektivitetsperspektiv och den utmynnade i rapporten *It-stödet i rättskedjan*[5]. Av rapporten framgår att de budgeterade IT-kostnaderna för de granskade myndigheterna 2011 uppgick till cirka 2,26 miljarder, varav polisen stod för närmare 70 procent av kostnaderna. I kostnaderna ingick drift, förvaltning, utveckling och avskrivningar för materiella och immateriella anläggningstillgångar.

Datainspektionens tillsyn

Tillsyn av RIF

Datainspektionen ska genom sin tillsynsverksamhet granska behandlingen av personuppgifter så att den inte leder till otillbörliga intrång i enskilda individers personliga integritet.

Straffet, som är samhällets reaktion mot ett oacceptabelt beteende, utgör i sig ett intrång i den personliga integriteten. Samtidigt upplevs ofta brottet som mycket kränkande av brottsoffret, men det kan också vara besvärande för brottsoffret att berätta om vad som hänt. Vittnet kan uppfatta både brottet och tvånget att berätta om händelsen som kränkande. Det innebär att brottmålsprocessen inte sällan upplevs som integritetskänslig av många av de berörda, men ur olika aspekter. De uppgifter som hanteras om dessa personer kräver därför försiktighet för att det inte ska ske något otillbörligt intrång i enskilda individers personliga integritet.

Den elektroniska överföringen mellan myndigheterna i rättskedjan har givetvis fördelar ur effektivitets synpunkt, men medför samtidigt att det blir enklare att sammanställa och söka uppgifter om enskilda personer och kartlägga deras liv och leverne. Inom rättsväsendet arbetar många personer och många av dem har behörighet till något system som ingår i RIF. Det innebär att det är många användare av systemen och de behandlar stora mängder integritetskänsliga personuppgifter. Det är därför viktigt att de regler som gäller till skydd för den personliga integriteten beaktas i RIF-arbetet.

5 Riksrevisionens rapport RIR 2011:25 It-stödet i rättskedjan

Riksrevisionen anger också i sin rapport att myndigheternas registerförfattningar, som reglerar personuppgiftsbehandlingen, inte ger tillräckliga förutsättningar för att utveckla IT-stödet i rättskedjan och att en samlad analys av lagstiftningen saknas.[6] Det är ytterligare ett skäl att granska arbetet i RIF utifrån reglerna som finns till skydd för den personliga integriteten.

Genomförande

Datainspektionen har under 2012 genomfört ett tillsynsprojekt som omfattar de sju myndigheter som ingår i den första etappen av RIF – RPS, ÅM, DV, EBM, SKV och Brå. Granskningen har inriktats på hur de regler som avser behandling av personuppgifter beaktas när uppgifter överförs mellan myndigheterna i RIF7 eller när uppgifterna görs tillgängliga för en annan myndighet inom RIF7.

Beslut om tillsyn har fattats för var och en av RIF7-myndigheterna.[7] Tillsynen av de sju myndigheter har huvudsakligen skett i enkätform. Alla myndigheterna har fått svara på två enkäter. Den ena enkäten har rört generella frågor om myndigheten och den andra har avsett de system som myndigheten använder för att behandla personuppgifter i brottmålsprocessen och där personuppgifterna överförs mellan ett par eller flera myndigheter i RIF7. Enkätsvaren har sammanställts och myndigheterna har beretts möjlighet att lämna synpunkter och komplettera uppgifterna. Förutom enkäterna har möte också ägt rum med SI-enheten på Justitiedepartementet, både inför och under tillsynen.[8] Sökningar har också gjorts vid vad som kallas *Allmänhetens terminal* vid Stockholms tingsrätt. Beslut har fattats i tillsynsärendena den 13 november 2012.

Denna rapport har sammanställts i ett gemensamt ärende.[9] Rapporten innehåller redogörelse för uppgifter som framkommit vid tillsynen och relevanta rättsregler. Rapporten avslutas med Datainspektionens bedömning av om myndigheterna i RIF7 i sitt arbete med att skapa ett elektroniskt informationsflöde på ett tillfredsställande sätt bevakar att personuppgifter inte behandlas på ett sätt som leder till otillbörliga intrång i enskilda individers personliga integritet.

Det bör redan här påpekas att RPS och DV i tillsynen svarat för system som utvecklas och förvaltas av dem, men som huvudsakligen har andra

6 Riksrevisionens rapport RIR 2011:25 It-stödet i rättskedjan s. 78-82

7 Beslut 2012-03-09 i Datainspektionens ärende dnr 419-2012 SKV, dnr 420-2012 RPS, dnr 421-2012 ÅM, dnr 422-2012 Brå, dnr 423-2012 KV, dnr 424-2012 EBM och dnr 425-2012 DV

8 Möte den 2011-10-24 och 2012-09-18 (Enheten för samordning, utveckling och informationsförsörjning)

9 Datainspektionens ärende dnr 418-2012

myndigheter som användare. För RPS del är det främst polismyndigheterna som är användare av systemen och beträffande DV är det de allmänna domstolarna.

Regler till skydd för den personliga integriteten

Regeringsformen, Europakonventionen och EU:s stadga om de grundläggande rättigheterna

Den offentliga makten ska utövas med respekt för bland annat den enskildes frihet och värdighet enligt *1 kap. 2 § regeringsformen.* I samma bestämmelse anges det också att det allmänna ska värna den enskildes privatliv. Dessutom finns det numera ett uttryckligt skydd för den personliga integriteten i *2 kap. 6 § andra stycket regeringsformen,* som lyder*;*

> *... är var och en gentemot det allmänna skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden*

För att inskränka denna rättighet krävs det enligt *2 kap. 20 § första stycket 2 punkten* och *21 § RF* att det sker med stöd i lag och att ändamålen ska vara godtagbara i ett demokratiskt samhälle. Begränsningen får dessutom aldrig gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den.

Enligt *artikel 8 i Europakonventionen* har var och en rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. Denna rättighet får inte inskränkas av det allmänna annat än med stöd av lag och om det i ett demokratiskt samhälle är nödvändigt med hänsyn till vissa närmare angivna ändamål.

EU:s stadga om de grundläggande rättigheterna (EU:s rättighetsstadga) beskriver de fri- och rättigheter som EU erkänner att varje människa har. Det handlar till exempel om tanke-, religions-, yttrande- och mötesfrihet, rätt till ett skyddat privatliv och barns rätt till skydd och omvårdnad. Stadgan är till stor del en sammanfattning av de rättigheter som redan finns inom EU genom fördragen och EU-domstolens praxis. *EU:s rättig-*

hetsstadga är juridiskt bindande sedan den 1 december 2009 då Lissabonfördraget började gälla. Skyddet av personuppgifter återfinns i *artikel 8* i stadgan och lyder:

1. *Var och en har rätt till skydd av de personuppgifter som rör honom eller henne.*
2. *Dessa uppgifter ska behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund. Var och en har rätt att få tillgång till insamlade uppgifter som rör honom eller henne och att få rättelse av dem.*
3. *En oberoende myndighet ska kontrollera att dessa regler efterlevs.*

Enligt *artikel 52* ska begränsningar i utövandet av de rättigheter och friheter vara föreskriven i lag och förenlig med det väsentliga innehållet i dessa rättigheter och friheter. Begränsningar får, med beaktande av proportionalitetsprincipen, endast göras om de är nödvändiga och faktiskt svarar mot mål av allmänt samhällsintresse som erkänns av unionen eller behovet av skydd för andra människors rättigheter och friheter.

Dataskyddskonventionen

Sverige ska också följa *Europarådets konvention från 1981 om skydd för enskilda vid automatisk databehandling av personuppgifter,* förkortad *Dataskyddskonventionen*. Konventionen kan ses som en precisering av *artikel 8* i *Europakonventionen* vad gäller skyddet för enskilda vid automatiserad behandling av personuppgifter.

I konventionen anges att personuppgifter som är föremål för automatisk databehandling ska hämtas in och behandlas på ett korrekt sätt för särskilt angivna ändamål. Uppgifterna ska vara relevanta för ändamålen och får inte heller senare användas på ett sätt som är oförenligt med dem. Uppgifterna måste också vara riktiga och aktuella och de får inte bevaras längre tid än vad som är nödvändigt för ändamålen. Vissa typer av personuppgifter får, enligt konventionen, behandlas endast om den nationella lagstiftningen ger ett ändamålsenligt skydd. Till sådana personuppgifter hör uppgifter som avslöjar ras, politisk tillhörighet, religiös tro eller övertygelse i övrigt, hälsa, sexualliv och uppgifter om brott. För att skydda personuppgifter mot förstörelse föreskriver konventionen att lämpliga skyddsåtgärder ska vidtas. Den registrerade ska också ha möjlighet till insyn i registret och rätt att få felaktiga uppgifter rättade. I vissa fall får undantag göras från konventionen, bland annat får undantag göras från bestämmelserna som gäller uppgifternas beskaf-

fenhet och rätten till insyn. Sådana inskränkningar förutsätter, enligt konventionen, stöd i den nationella lagstiftningen och att inskränkningen är nödvändig i ett demokratiskt samhälle för vissa angivna ändamål, till exempel statens ekonomiska intressen och brottsbekämpning, samt för att skydda enskildas fri- och rättigheter.

Dataskyddsdirektivet och dataskyddsrambeslutet

För att garantera en likvärdig och hög skyddsnivå i alla medlemsländer inom EU antogs 1995 *Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (dataskyddsdirektivet).* Direktivet, som utgör en precisering och förstärkning av principerna i *dataskyddskonventionen,* undantar bland annat den brottsbekämpande verksamheten från sitt tillämpningsområde. Inom detta område finns istället *Rådets rambeslut 2008/977/RIF av den 27 november 2008 om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete (dataskyddsrambeslutet). Dataskyddsrambeslutet* rör behandling av personuppgifter som överförs mellan länderna på det brottsbekämpande verksamheter. Rambeslutet förpliktar medlemsstaterna att behandla sådana personuppgifter som utbyts mellan staterna på visst sätt för att förstärka skyddet för denna typ av information inom det straffrättsliga området. När regeringen skulle överväga vilka lagändringar som rambeslutet krävde, konstaterades att rambeslutet i stora delar motsvarar *dataskyddsdirektivet*, som har genomförts i svensk rätt genom *personuppgiftslagen (1998:204).*[10]

Personuppgiftslagen

Personuppgiftslagen (1998:204) förkortad *PuL* syftar till att skydda enskilda personer mot kränkning av den personliga integriteten vid behandling av personuppgifter på automatiserad väg eller i manuella personregister som uppfyller vissa kriterier. *PuL* grundar sig på *dataskyddsdirektivet,* men till skillnad från direktivet har den brottsbekämpande verksamheten inte undantagits från lagens tillämpningsområde.

I *3 § PuL* definieras *personuppgifter* som all slags information som direkt eller indirekt kan hänföras till en fysisk person i livet och *behandling* omfattar alla åtgärder som vidtas med uppgifterna. Även att ta del av en personuppgift är att betrakta som en behandling av uppgiften.

10 Prop. 2008/09:16 Godkännande av dataskyddsrambeslutet

Personuppgiftsansvarig är den som ensam eller tillsammans med andra bestämmer ändamålet med eller medlen för behandlingen.

Lagen bygger i likhet med direktivet på den restriktiva tekniken att först förbjuda all behandling av personuppgifter för att sedan räkna upp de fall där behandlingen trots allt är tillåten.[11]

För att underlätta vardagliga behandlingar av personuppgifter har *PuL* sedan 2007 två olika regelsystem. Det ena gäller material som är ordnat i register och andra samlingar där personuppgifterna har strukturerats för att påtagligt underlätta sökning efter eller sammanställning av personuppgifter. Exempel på det är traditionella dataregister, databaser och ärende- och dokumenthanteringssystem. Det andra regelsystemet omfattar ostrukturerat material som inte har någon mer avancerad struktur eller sökbarhet, som till exempel fritext, bilder och listor på personer. Definitionen av ostrukturerat material återfinns i *5 a § PuL*. I ostrukturerat material tillåts i princip all behandling av personuppgifter så länge den inte kränker den person som uppgiften avser, enligt den så kallade *missbruksregeln* i *5 a § andra stycket PuL*.

För behandling av personuppgifter i ett strukturerat material gäller de så kallade hanteringsreglerna i *PuL*. I hanteringsreglerna ingår de grundläggande kraven för behandling av personuppgifter i *9 § PuL*, regler om när personuppgiftsbehandling är tillåten *10 §*, regler i *13–19 §§* om behandling av känsliga personuppgifter, förbud för andra än myndigheter att behandla uppgifter om brott *21 §*, bestämmelser om information till den registrerade *23–26 §§*, regler om rättelse *28 §* och bestämmelser om överföring av personuppgifter till tredje land *33–34 §§*.

Fritext eller bilder som normalt är att bedöma som ostrukturerat material, ska följa reglerna för strukturerat material om de ingår eller är avsedda att ingå i en strukturerad samling av personuppgifter. I förarbetena till *5 a § PuL* uttrycktes det enligt följande.[12]

> *Om materialet som sådant, dvs. hela samlingen av uppgifter, har strukturerats så att hanteringsreglerna är tillämpliga, skall hanteringsreglerna tillämpas vid behandling av alla personuppgifter – strukturerade och ostrukturerade – som finns i materialet oavsett om vissa personuppgifter i materialet inte har strukturerats. Personuppgifterna kan nämligen finnas till exempel i ordbehandlingsdokument, i inskannade dokument och i ljud- och bildupptagningar som i och för sig*

11 Personuppgiftslagen En kommentar, Öman och Lindblom uppl. 4:1 s. 12
12 Prop. 05/06:173 s.23

kan vara ostrukturerade men som ingår i den strukturerade samlingen av uppgifter, till exempel ett ärendehanteringssystem. Det är själva samlingen av uppgifter som skall vara strukturerad på visst sätt, inte varje personuppgift eller handling som ingår i samlingen.

De särskilda registerförfattningarna

PuL är subsidiär till andra författningar. Det framgår av *2 § PuL* som anger att om det i lag eller förordning finns bestämmelser som avviker från denna lag ska de bestämmelserna gälla. Många myndigheter har särskilda författningar som reglerar personuppgiftsbehandlingen i just deras verksamhet. Dessa så kallade s*ärskilda registerförfattningar* kan innebära både större tillåtlighet att behandla personuppgifter, men också vara strängare än *PuL*. En del registerförfattningar gäller tillsammans med *PuL* och en del gäller istället för *PuL*. Det råder stor variation mellan olika registerförfattningar och varje myndighet måste kontrollera att den behandling av personuppgifter som sker stämmer överens med de regler som gäller för den egna verksamheten. I avsnittet nedan där myndigheterna presenteras anges de i detta sammanhang mest relevanta registerförfattningarna för respektive myndighet.

Det är problematiskt att de *särskilda registerförfattningarna* skiljer sig så mycket från varandra. Regeringen har uppmärksammat detta och det pågår en utredning som har fått i uppdrag av regeringen att bland annat utarbeta en generell modell för reglering av registerfrågor.[13] Ambitionen att få registerförfattningarna att mer likna varandra syns inte minst på rättsväsendets område, se *polisdatalagen (2010:361)* och *kustbevakningsdatalagen (2012:145).* Även de förslag till nya registerförfattningar som för närvarande bereds på Justitiedepartementet gällande domstols- och åklagarväsendet har liknande uppbyggnad.[14]

Kommissionens förslag

Det pågår även förändringar på en mer grundläggande nivå. Den europeiska kommissionen har i början av året presenterat ett förslag till en *dataskyddsförordning*[15] som föreslås ersätta *dataskyddsdirektivet* och för Sveriges del även *PuL*.

På det brottsbekämpande området föreslås istället ett direktiv *Kommissionens förslag till dataskyddsdirektiv för de brottsbekämpande myndig-*

13 Kommittédirektiv 2011:86 Integritet, effektivitet och öppenhet i en modern e-förvaltning

14 SOU 2001:100 Informationshantering och behandling av uppgifter vid domstolar – En rättslig översyn och SOU 2008:87 Åklagarväsendets brottsbekämpning, Integritet – Effektivitet

15 Kommissionens förslag till dataskyddsförordning (KOM (2012) 11 slutlig)

heterna.[16] Direktivet ska enligt *artikel 1.1* gälla för behandling av personuppgifter som utförs av behöriga myndigheter i syfte att förebygga, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder och kommer därför att omfatta de myndigheter som är involverade i brottmålsprocessen.

Några av kommissionens förslag i direktivet kan vara värda att notera i sammanhanget. Kommissionen föreslår till exempel att det ska göras åtskillnad på olika kategorier av registrerade personer. I *artikel 5* föreslår kommissionen fem kategorier. Den första består av personer som med styrka kan misstänkas ha begått eller vara på väg att begå brott. Andra kategorin består av de som dömts eller på annat sätt lagförts. Den tredje består av brottsoffer och den fjärde omfattar närmast vittnen, sakkunniga och anhöriga. Den femte och sista kategorin består av övriga personer. När personuppgifter behandlas ska enligt förslaget, kategorin framgå på ett noggrant och tillförlitligt sätt så långt det är möjligt. Känsliga personuppgifter får inte behandlas enligt huvudregeln i *artikel 8* i förslaget. Från huvudregeln föreslås det undantag. Av störst betydelse i detta sammanhang är undantaget som anger att känsliga personuppgifter får behandlas om behandlingen tillåts i en lag som också föreskriver lämpliga skyddsåtgärder. Den personuppgiftsansvarige ska, med hänsyn till vad som är tekniskt och ekonomiskt möjligt, använda lämpliga tekniska och organisatoriska åtgärder för att säkerställa att behandlingen av personuppgifter överensstämmer med kraven i de bestämmelser som antas enligt direktivet. Det anges i *artikel 19* i förslaget och kallas *”Data protection by design”*.

Myndigheterna i RIF 7

Rikspolisstyrelsen (RPS)

RPS är en central förvaltningsmyndighet för polisväsendet med ansvar för samordning och rationalisering av polisväsendet och fördelning av de statliga medlen till polismyndigheterna. Polisväsendet består av RPS och 21 fristående myndigheter som är geografiskt spridda över landet. Säkerhetspolisen och Rikskriminalpolisen tillhör RPS. I betänkandet *En sammanhållen svensk polis SOU 2012:13* föreslås att RPS, Statens kriminaltekniska laboratorium och de 21 polismyndigheterna ombildas till en

16 Kommissionens förslag till dataskyddsdirektiv för de brottsbekämpande myndigheterna (KOM (2012) 10 slutlig)

enda myndighet. Säkerhetspolisen föreslås bli en fristående myndighet. Hos polisen arbetar det sammanlagt cirka 28 000 personer.

Enligt *2 kap. 4 § polisdatalagen (2010:361)* är varje polismyndighet personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför.

Brottmålsprocessen inleds ofta hos polisen. Det är polisens uppgift att ta emot och upprätta anmälningar om brott. Polisen utreder också brott. Det kan ske under egen ledning eller under förundersökningsledning av en åklagare. I utredningar som polisen själva är förundersökningsledare för, ska polisen bedöma om det föreligger tillräckliga skäl för åtal och i så fall redovisas ärendet till åklagare. Polisen får även utfärda ordningsbot beträffande brott som har penningböter i straffskalan och där ett belopp för ordningsbot bestämts av riksåklagaren.

RPS har också fått i uppgift att föra ett antal register som inte direkt är relaterade till polisens egen verksamhet. Av intresse i detta sammanhang är misstankeregistret (MR), belastningsregistret (BR) och rättsväsendets informationssystem (RI-systemet). Den del av RI-systemet som RPS är personuppgiftsansvarig för är den som behandlar domar och slutliga beslut i brottmål och brottsanmälningar. RI-systemet skapades i början av 70-talet och bestämmelserna som reglerar personuppgiftsbehandlingen i RI-systemet återfinns i *förordningen (1970: 517) om rättsväsendets informationssystem*. Ett av målen i den första etappen av RIF är att fasa ut RI-systemet och systemet i sig själv har därför utelämnats från tillsynen.

Polisen har fem system utöver RI–systemet som är involverade i brottmålsprocessen och som omfattas av det elektroniska informationsflödet som avses i RIF.

- Rationell anmälansrutin (RAR)
- Datoriserad utredningsrutin med tvångsmedel (DurTvå)
- Polisens Utredningsstöd (Pust)
- Misstankeregistret (MR)
- Belastningsregistret (BR)

Personuppgiftsbehandlingen i polisens brottsbekämpande verksamhet regleras i *polisdatalagen (2010:361)* och *polisdataförordningen (2010:1155)*. Polisen har också en intern föreskrift som är tillämplig, *Rikspolisstyrelsens föreskrifter och allmänna råd om behandling av personuppgifter i Polisens brottsbekämpande verksamhet (RPSFS 2011:11, FAP 171-3)*. Polisda-

talagen gäller istället för *PuL (1998:204) (PuL)* undantaget de bestämmelser i *PuL* som i *2 kap. 2 § polisdatalagen* anges vara tillämpliga. Beträffande den personuppgiftsbehandling som sker i polisens verksamhet och som inte avser polisens brottsbekämpande verksamhet, såsom hjälpande verksamhet och verksamhet för att upprätthålla ordning och säkerhet, är *PuL* tillämplig. För MR gäller *lagen (1998:621) om misstankeregistret* och *förordningen (1999: 1135) om misstankeregistret*. Även BR omfattas på samma sätt av en egen reglering *lagen (1998:620) om belastningsregistret* och *förordningen (1999: 1134) om belastningsregistret*.

Åklagarmyndigheten (ÅM)

ÅM leds av riksåklagaren och myndighetens operativa verksamhet bedrivs av 39 åklagarkamrar som är spridda över hela landet. ÅM har ungefär 1 400 personer anställda varav ungefär 900 är åklagare.

Åklagarens huvuduppgift är att utreda brott, fatta beslut om åtal ska väckas eller inte och föra talan i domstolen. Åklagaren leder förundersökningar när det inte är frågan om enklare brott. Polisen utreder brott på uppdrag av åklagaren och efter åklagarens anvisningar (direktiv). Om åklagaren bedömer att det går att styrka att den misstänkte begått ett brott väcker åklagaren åtal i en allmän domstol. I domstolen är det åklagaren som för talan mot den åtalade. Istället för att väcka åtal kan åklagaren i vissa fall utfärda strafföreläggande (böter) eller meddela åtalsunderlåtelse.

Det är i Cåbra (Centralt system för åklagarväsendets brottmålshantering) som diarieföring, hantering av handlingar och dokument skapas i den operativa verksamheten inom åklagarväsendet.

För ÅM:s personuppgiftsbehandling gäller utöver *PuL*, *förordningen (2006:937) om behandling av personuppgifter inom åklagarväsendet*.

Ekobrottsmyndigheten (EBM)

EBM bildades 1998 och är en åklagarmyndighet som bedriver både polis- och åklagarverksamhet. EBM har som uppgift att utreda och lagföra ekonomisk brottslighet huvudsakligen i de tre storstadsregionerna.

Inom EBM arbetar ungefär 430 personer och verksamheten bedrivs i Stockholm, Göteborg och Malmö och dessutom vid ett antal utredningsenheter placerade i Visby, Halmstad, Borås, Skövde, Karlskrona och Kristianstad. I betänkandet *En samlad ekobrottsbekämpning (SOU 2011:47)* föreslås att verksamheten ska bli rikstäckande.

De poliser som arbetar vid EBM är anställda av Rikskriminalpolisen som är en avdelning under RPS. Poliserna förordnas med stöd av *8 § förordningen (2007:972) om instruktion för Ekobrottsmyndigheten* att tjänstgöra vid EBM.

I det operativa arbetet använder EBM som verksamhetsstöd Cåbra, RAR och DurTvå. Det är således ÅM:s och polisens system som EBM använder, medan ÅM och RPS fortfarande ansvarar för förvaltning, utveckling och lagring av uppgifter. Systemen används på ett annat sätt hos EBM. Eftersom brotten oftast utreds av poliser som tjänstgör vid EBM, blir det hos EBM inte frågan om någon överföring av uppgifter från myndighet till myndighet mellan RAR, DurTvå och Cåbra. Hos EBM används inte heller RAR och DurTvå för att kommunicera med andra system externt. Det innebär till exempel att EBM enbart levererar uppgifter till MR och till Brå:s system SOR från Cåbra. Eftersom den här tillsynen avser de system som överför personuppgifter mellan myndigheterna i brottmålsprocessen granskas för EBM:s del enbart Cåbra. Trots det kommer det i avsnittet om *Myndigheternas personuppgiftsansvar* beröras något om omfattningen av RPS personuppgiftsansvar i de system som används av EBM.[17] EBM följer samma regelverk som ÅM beträffande Cåbra.

Domstolsverket (DV)

DV utgör tillsammans med de allmänna domstolarna, de allmänna förvaltningsdomstolarna, hyres- och arrendenämnderna och Rättshjälpsmyndigheten *Sveriges Domstolar*. DV:s roll är att ge administrativt stöd och service åt domstolarna och nämnderna. Inom verksamhetsområdet ska DV i administrativt hänseende leda och samordna verksamheten för att skapa förutsättningar för att den bedrivs rättssäkert och effektivt.

Sveriges Domstolar har sammanlagt ungefär 6 500 anställda och verksamheten är geografiskt spridd över landet. Varje domstol och nämnd utgör en egen myndighet och bestämmer själva över sin organisation.

Det är de allmänna domstolarna som dömer i brottmål som huvudsakligen är involverade i brottmålsprocessen. De allmänna domstolarna bestod vid utgången av år 2011 av 48 tingsrätter, sex hovrätter och Högsta domstolen. Under år 2011 hade de allmänna

17 2 kap. 4 § polisdatalagen (2010:361)

domstolarna i medeltal totalt 3 880 anställda. De allmänna domstolarna handlägger även andra mål och ärenden förutom brottmål.

I den rättsskipande eller rättsvårdande verksamheten sker domstolarnas och nämndernas registerföring i verksamhetsregister genom det elektroniska verksamhetsstödet Vera. Varje domstol har sitt eget verksamhetsregister.

Personuppgiftsbehandlingen som avser brottmålsprocessen regleras utöver *PuL* för de allmänna domstolarna främst i *förordningen (2001:639) om registerföring m.m. vid allmänna domstolar med hjälp av automatiserad behandling*.

Kriminalvården (KV)

KV ansvarar för att verkställa utdömda påföljder, bedriva häktesverksamhet och utföra personutredningar i brottmål. KV har också en omfattande transporttjänst av frihetsberövade.

KV har omkring 10 800 anställda och verksamheten är spridd över landet.

De personuppgifter som överförs i rättskedjan behandlas inom KV i Kriminalvårdsregistret (KVR).

Lagen (2001:617) om behandling av personuppgifter inom kriminalvården och *förordningen (2001:682) om behandling av personuppgifter inom kriminalvården* reglerar KV:s personuppgiftsbehandling avseende personer som är föremål för personutredning, intagna i häkte, dömda till fängelse, skyddstillsyn, villkorlig dom med samhällstjänst eller som transporteras av KV:s transporttjänst (ytterligare kategorier finns men är av mindre intresse i detta sammanhang). Enligt lagens *2 §* ska *PuL* tillämpas vid behandling av personuppgifter inom KV om inte annat följer av den angivna lagen eller föreskrifter som meddelats med stöd av lagen.

Skatteverket (SKV)

SKV är en myndighet som huvudsakligen sysslar med beskattningsverksamhet. SKV ansvarar också för annan verksamhet såsom folkbokföring och det statliga personadressregistret. Verksamheten är uppdelade i sju skatteregioner och en organisatorisk region inriktad mot stora företag. Antalet anställda var 2011 ungefär 10 500.

SKV:s beskattningsverksamhet är involverad i brottmålsprocessen i egenskap av anmälare av brott i huvudsak skattebrott.

Inom SKV bedrivs också brottsbekämpande verksamhet inom särskilda enheter, skattebrottsenheter (SBE) som organisatoriskt är avskilda från den övriga verksamheten. SBE utför förundersökningar på uppdrag av åklagare och bedriver egen underrättelseverksamhet avseende ekonomisk brottslighet i enlighet med *lagen (1997: 1024) om Skatteverkets medverkan i brottsutredningar*. Det är cirka 250 personer som arbetar inom SBE.

SKV är mitt uppe i ett arbete med att utveckla två olika IT-system för att stödja den anmälande och den brottsutredande verksamheten. Systemen har arbetsnamnen RIF Brottsanmälan (BA) och RIF Brottsutredning (BU). Systemet BA för anmälningar har börjat driftsättas, medan BU beräknas att vara i drift till halvårsskiftet 2013.

För SKV är det olika registerförfattningar som gäller beroende på om behandlingen avser SKV:s anmälande eller brottsutredande verksamhet. Den anmälande verksamheten är, som beskrivits, en del av SKV:s beskattningsverksamhet och i den verksamheten ska därför *lagen (2001:1818) om behandling av uppgifter i skatteverkets beskattningsverksamhet* och *förordningen (2001:588) om behandling av uppgifter i skatteverkets beskattningsverksamhet* vid personuppgiftsbehandling. Lagen gäller om inte annat anges istället för *PuL*. I den brottsbekämpande verksamheten regleras personuppgiftsbehandlingen i *lagen (1999:90) om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar* och *förordningen (1999:105) om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar.* Denna lag gäller utöver *PuL* vid behandling av personuppgifter när SKV:s bedriver spaning, utreder brott eller arbetar brottsförebyggande.

Brottsförebyggande rådet (Brå)

Brå ingår egentligen inte i brottmålsprocessen. Brå har som uppdrag att bedriva forskning kring brottslighet och brottsförebyggande arbete och att producera Sveriges officiella kriminalstatistik och annan rättsstatistik. Statistikuppdraget innebär att Brå ska ta fram statistik över anmälda brott, misstänkta personer, uppklarade brott, för brott lagförda personer, narkotikabrott, kriminalvård och återfall i brott. Det är för att kunna fullgöra detta uppdrag och utveckla den officiella kriminal- och rättsstatistiken som Brå deltar i RIF-samarbetet. Brå är således enbart mottagare av information från rättsväsendet och har därför en särställning i denna granskning.

Brå har 95 anställda och verksamheten är samlad i Stockholm

Statistikuppgifterna registreras i Systemet för officiell rättsstatistik (SOR).

Brå har ingen verksamhetsspecifik registerlag att beakta. Den personuppgiftsbehandling som sker i Brå:s statistikverksamhet har stöd i *lagen (2001:99) om den officiella statistiken* och *förordningen (2001:100) om den officiella statistiken*. Av förordningen framgår att Brå är statistikansvarig myndighet på rättsväsendets område, med undantag för domstolarnas verksamhet.

En kortfattad beskrivning av aktuella system

RAR

RAR (Rationell anmälansrutin) är polisens system för att upprätta anmälan. Systemet togs i bruk 1991 och planeras att vara avvecklat vid utgången av 2014. Sammanlagt registreras cirka 1 400 000 anmälningar per år. Det är RPS som utvecklar och förvaltar systemet och som också svarar för lagringen av uppgifterna. RAR ska enligt planerna avvecklas.

DurTvå

DurTvå (Datoriserad utredningsrutin med tvångsmedel) togs i bruk 2000 och är polisens utredningsstöd. I DurTvå hanteras uppgifter som tillhör förundersökningen såsom anmälningar, förhör och sakkunnigutlåtanden. Även de tvångsmedel som används i förundersökningen antecknas i DurTvå. DurTvå är planerad att avvecklas samtidigt som RAR vid utgången av 2014. DurTvå har ungefär 25 000 användare och sammanlagt finns det i DurTvå 2,7 miljoner ärenden. Det är RPS som utvecklar och förvaltar systemet och som också svarar för lagringen av uppgifterna.

Pust

Polisens utredningsstöd Pust togs i bruk 2011 och är ett utredningsstöd som ska ersätta både RAR och DurTvå. Än så länge hanteras bara vissa mängdbrott i Pust, men Pust befinner sig i en utvecklingsfas där utredningar av olika typer av brott successivt ska föras in i Pust. Nästa

steg i utvecklingen är fas 2, i den ska brott mot person börja hanteras i Pust. I fas 3 ska förmögenhetsbrotten in i systemet. Därefter ska specialstraffrätten föras in. År 2015 ska all anmälnings- och utredningsverksamhet inom polisen hanteras i Pust. För närvarande pågår en flytt av Pust till en ny standardplattform som ska tas i drift i november 2012. Det är RPS som utvecklar och förvaltar systemet och som också svarar för lagring av uppgifter i Pust. När det gäller mängdbrotten är Pust anpassat för att användas ute på fältet med hjälp av mobila enheter.

RPS beräknar antalet användare av Pust till ungefär 27 000 fördelat på behörighetskategorierna utredare, förundersökningsledare och arkivarie. I Pust finns det cirka 62 000 personer registrerade men det kommer att utökas när fler brottstyper hanteras i systemet.

MR

Misstankeregistret (MR) är ett gemensamt register för rättsväsendet där de som nått misstankegraden *skäligen misstänkta* antecknas. Uppgifterna tas bort från MR om personen inte längre är misstänkt för brottet eller om han eller hon dömts eller på annat sätt lagförts för brottet. De är de myndigheter som kan besluta om misstankar eller lagföring som levererar uppgifter till MR. Registret togs i bruk år 2000 och antalet registrerade är cirka 91 000.

RPS har enligt *lagen (1998:621) om misstankeregister* i uppgift att föra registret och det är RPS som svarar för utveckling, förvaltning och lagring av uppgifterna och som dessutom är personuppgiftsansvarig för behandlingen av personuppgifterna i registret.

BR

BR är på samma sätt som MR ett gemensamt register för rättsväsendet. I registret antecknas huvudsakligen personer som dömts eller på annat sätt lagförts för brott eller som erhållit kontakt- eller tillträdesförbud. Registret togs i bruk år 2000 och antalet registrerade är cirka 1,6 miljoner.

Registret förs med stöd av *lagen (1998:620) om belastningsregister* och *förordningen (1999: 1134) om belastningsregister.* RPS har enligt lagen som uppgift att föra registret och RPS är också personuppgiftsansvarig för behandlingen av personuppgifterna i registret. RPS svarar också för utveckling, förvaltning och lagring av uppgifterna.

Cåbra

Cåbra är förkortning för Centralt system för åklagarväsendets brottmålshantering och används för diarieföring och ärendehantering inom åklagarverksamheten. Systemet togs i bruk 2007 och regleras i *förordningen (2006:937) om behandling av personuppgifter inom åklagarväsendet*. Att det är åklagarväsendets system innebär att både ÅM och EBM använder det, men det är ÅM som ansvarar för utveckling och förvaltning av systemet. Det är också ÅM som lagrar uppgifterna. Enligt ÅM har totalt med EBM cirka 1 600 personer behörighet till Cåbra. Hos ÅM har samtliga åklagare och administratörer behörighet till Cåbra. Hos EBM är 185 personer behöriga och det är åklagare, ekoadministratörer, IT-samordnare och analytiker. Polisen som tjänstgör hos EBM har inte behörighet till Cåbra eftersom de inte är anställda av EBM. Kvantitetsmässigt uppger ÅM att de 2011 hanterade 210 438 ärenden i Cåbra. EBM anger för samma år att de har 4 900 inkomna ärenden. I vart och ett av ärendena i Cåbra behandlas ett flertal personuppgifter.

Vera

De allmänna domstolarnas registerföring sker, i den rättsskipande eller rättsvårdande verksamheten, i verksamhetsstödet Vera. Vera driftsattes successivt under perioden 2003–2004. DV har utvecklat Vera och systemet förvaltas av DV och domstolarna. Lagringen av uppgifter sker hos DV.

Domstolarna avgör vilka som ska ha tillgång till Vera och DV saknar därför uppgift om antalet användare. DV antar dock att i princip samtliga anställda vid Sveriges domstolar har någon form av behörighet i Vera. En realistisk uppskattning ger då vid handen att det totalt finns något över 6 000 användare av Vera.

Beträffande antalet personuppgifter i Vera kom det under år 2011 in 90 929 brottmål till tingsrätterna, 9 527 brottmål till hovrätterna och 1 807 brottmål till Högsta domstolen. I vart och ett av brottmålen finns det registrerat uppgifter om minst en tilltalad. Härutöver finns exempelvis uppgifter om åklagare, försvarare, målsäganden och vittnen registrerade i varierande omfattning.

KVR

Kriminalvårdsregistret (KVR) togs i bruk 2003 och omfattar i huvudsak uppgifter om personer som är föremål för personutredning, intagna i häkte, dömda till fängelse, skyddstillsyn, villkorlig dom med samhällstjänst eller personer som transporteras av KV:s transporttjänst. Behand-

lingen av personuppgifter regleras *av lagen (2001:617) om behandling av personuppgifter inom kriminalvården* och *förordningen (2001:682) om behandling av personuppgifter inom kriminalvården*.

KVR har funnits länge som system men funktionerna har utökats och håller fortfarande på att utökas. Uppgifter som tidigare hanterades i systemet FRAS (Frivårdens Administrativa System) hanteras numera i KVR och FRAS är avvecklat. Även systemet KLAS (Klient Administrativa System) håller på att avvecklas och när det är klart 2014 ska alla uppgifterna från KLAS också behandlas i KVR.

I KVR finns 200 000 personer registrerade. KV uppskattar att varje person har överstigande 1000 poster. Behörighet att använda KVR har alla inom KV med klientkontakt och det har cirka 10 000 personer, det vill säga merparten av de som arbetar inom KV.

RIF Brottsanmälan och Brottsutredning (arbetsnamn)

SKV har inom brottsbekämpning idag två olika system som är under utveckling med arbetsnamnen RIF Brottsanmälan (BA) och RIF Brottsutredning (BU).

SKV anmäler varje år cirka 4 000 brott och dessa anmälningar kommer att ske via systemet BA. BA ska också ta emot uppföljningsinformation i syfte att utöva tillsyn, kontroll, uppföljning och planering av verksamheten. Personuppgiftsbehandlingen regleras i *lagen (2001:181) om behandling av uppgifter i Skatteverkets beskattningsverksamhet* och *förordningen (2001:588) om behandling av uppgifter i Skatteverkets beskattningsverksamhet*. I *1 kap. 2 §* i nämnda lag anges att den gäller istället för *PuL*. BA driftssätts under denna höst 2012. SKV uppskattar att 2 300 personer kommer att få någon form av behörighet till systemet.

Skattverkets brottsutredandeverksamhet SBE genomför cirka 2 000 förundersökningar varje år. Utredningarna sker idag i ett utredningsstöd som kallas Sebra. Det är ett helt slutet system som inte kommunicerar utanför SKV. Sebra ska under våren 2013 ersättas med systemet BU. Personuppgiftsbehandlingen regleras i *lagen (1999:90) om behandling av personuppgifter i Skatteverkets medverkan i brottsutredningar* och *förordningen (1999:105) om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar.* Denna lag gäller enligt dess *1 §* utöver *PuL*. SKV anger att ungefär 250 personer kommer att ha behörighet till BU.

SOR

I Systemet för officiell rättsstatistik (SOR) lagrar Brå uppgifter om misstankar om brott, lagföring och verkställighet för att kunna producera den officiella rättsstatistiken. SOR är uppbyggt av tre delar – en mottagande, en för kontroll och en del som innehåller långtidslagring av indata. I den mottagande delen speglas exakt den information som de avrapporterande systemen skickar till Brå. Den information som Brå erhåller är inte alltid tillfyllest för myndighetens syfte att producera statistik. Därför mellanlagras informationen i kontrollstationen där de enskilda ärendena kan kontrolleras. Det innebär att Brå bedömer om informationen kan användas som underlag för en rättvisande statistik. I de fall Brå upptäcker brister i informationens kvalitet rättas den. Det sker vanligtvis genom att Brå konsulterat källan. Den upprättade informationen flyttas sedan till långtidslagringen. När informationen är placerad i långtidslagringen ska den som huvudregel inte ändras.

Brå har ingen verksamhetsspecifik registerlag att beakta. Den personuppgiftsbehandling som sker i Brå:s statistikverksamhet har stöd i *lagen (2001:99) om den officiella statistiken* och *förordningen (2001:100) om den officiella statistiken*.

En kvantitativ beskrivning av antal personuppgifter kan Brå inte ge. Det finns uppgifter från 1973 och framåt. Uppgifterna gallras aldrig. Mängden uppgifter är därför mycket omfattande. Hos Brå har 24 personer behörighet till systemet.

Brottmålsprocessen – ett exempel

Rättskedjan innebär såsom ordet antyder att verksamheterna hänger samman. De olika aktörerna i brottmålsprocessen har väl definierade uppgifter som länkar i varandra. Samma uppgifter behandlas därför i brottmålsprocessen av flera myndigheter. Det kan ske i tur och ordning, men också parallellt . Uppgifterna kan också överföras vid flera tillfällen och i olika riktningar. För att åskådliggöra brottmålsprocessen ges nedan ett exempel på ett brottmål och hur personuppgifterna sprids till myndigheterna i RIF7. I exemplet redogörs inte för alla överföringar som kan förekomma utan endast huvuddragen.

Adam driver ett företag och vid en skatterevision blir han misstänkt för att ha begått skattebrott. Skatteverket anmäler misstankarna till EBM.

Några månader senare anmäls Adam också till polisen för att ha allvarligt misshandlat en man som Adam haft en kortvarig sexuell relation med. Denna person arbetar inom rättsväsendet. Adam anhålls och häktas misstänkt för grov misshandel. I tingsrätten fälls Adam för misshandel och skattebrott. Målet överklagas. I hovrätten frias Adam från skattebrottet, men den fällande domen för misshandel kvarstår. Adam döms till två månaders fängelse.

Adams ärende börjar således med att skattebrottet anmäls av SKV:s fiskala verksamhet till EBM. Anmälan kommer att hanteras i SKV:s system *BA*. Hos EBM inleds ett ärende i *Cåbra* där anmälan och bifogade uppgifter från BA hanteras. Brottsutredningarna i EBM:s ärenden sker antingen av de poliser som är förordnade att tjänstgöra hos EBM eller av SBE hos SKV. I Adams fall är det SBE som får uppdraget att utreda brottet. Utredningen sker nu i *Sebra* men kommer framöver att ske i SKV:s system *BU*. Lämnar åklagaren en begäran till tingsrätten att Adam vill ha en offentlig försvarare kommer uppgifterna om Adam och brottet även att behandlas i *Vera*. Från *Cåbra* skickas uppgifter till *MR* om att Adam är misstänkt för skattebrott. Även Brå:s system *SOR* får uppgifter från *Cåbra* om misstanken om skattebrott. Brå använder uppgifterna till den officiella rättsstatistiken, men där återfinns uppgifterna bara i anonym form. Eftersom RPS ansvarar för *MR* och att ÅM lagrar och har tillgång även till EBM:s uppgifter i *Cåbra*, är alla myndigheter i RIF 7 utom KV inblandade i personuppgiftshanteringen redan i och med att Adam anmäls för skattebrott, en förundersökning inleds med Adam som misstänkt och en offentlig försvarare begärs.

Adam anmäls sedan som misstänkt för grov misshandel. Anmälan sker hos polisen som registrerar anmälan i *RAR*. Utredningen hanteras därefter i *DurTvå*. Om ett par år kommer polisen hantera både anmälan och utredningen i *Pust*. Förundersökningen leds av en åklagare som hanterar ärendet i *Cåbra*. Från *DurTvå* skickas uppgifter direkt till *Cåbra*. Även dessa misstankar överförs till *MR* och *SOR*. Åklagaren begär sedan Adam häktad hos tingsrätten och uppgifterna om den grova misshandeln behandlas i *Vera*. KV får uppgifter om Adam av flera olika skäl. Uppgifterna rörande Adam behandlas i *KVR* för att han är frihetsberövad och placerad hos KV, för att han som frihetsberövad transporteras av KV och för att KV i sin frivårdsverksamhet utför en personutredning avseende Adam. Under förundersökningen av den grova misshandeln är därför alla RIF7-myndigheterna utom SKV och EBM involverade.

Förundersökningarna ska sedan slutföras. SBE sammanställer ett förundersökningsprotokoll gällande skattebrottet i *BU* och skickar det till

EBM som hanterar det i *Cåbra*. Polismyndigheten sammanställer i *DurTvå* ett förundersökningsprotokoll gällande den grova misshandeln som skickas till *Cåbra* hos ÅM. Åklagarna på EBM respektive ÅM väcker åtal. Det innebär att från *Cåbra* skickas stämningsansökan och förundersökningsprotokoll till *Vera* hos tingsrätten. I Adams fall beslutar tingsrätten att gärningarna ska hanteras i en och samma rättegång.

Tingsrätten inhämtar från KV en personutredning gällande Adam. Åklagaren får del av personutredningen inför huvudförhandlingen. Tingsrätten håller huvudförhandling och meddelar sedan dom. Uppgifter om domen rapporteras till *BR* och *RI-systemet*. Från *RI-systemet* distribueras domen vidare till bland annat Brå och KV. När *RI-systemet* avvecklats ska domen sändas direkt från domstolen istället. Åklagaren får som part del av domen från domstolen.

I detta fall överklagar Adam domen. Tingsrättens uppgifter om målet i *Vera* blir tillgängliga för hovrätten när målet överklagas och tingsrätten får samtidigt tillgång till hovrättens uppgifter. Hovrätten dömer Adam till två månaders fängelse för misshandel och friar honom för skattebrott. Även denna dom rapporteras till och distribueras via *RI-systemet*. När hovrättens dom vinner laga kraft gallras uppgifterna om Adam från *MR* genom att hovrätten lämnar uppgifter till ÅM som rapporterar dem direkt till *MR*. Domen rapporteras även till *BR*. KV rapporterar uppgifter om verkställigheten av fängelsestraffet till *BR* och till Brå.

Det innebär att i detta exempel har uppgifterna behandlats av alla RIF7-myndigheterna.

Elektronisk överföring av uppgifter inom rättsväsendet

Informationsutbyte i elektronisk form har förekommit mellan myndigheterna i rättskedjan under lång tid. Innan etapp 1 i RIF påbörjades har polisen, ÅM och EBM skickat uppgifter till MR och BR. Alla RIF7-myndigheter har också på olika sätt tillgång till MR och BR. Domstolarna skickar domar och slutliga beslut i brottmål till RPS för att hanteras i RI-systemet. Även polisens brottsanmälningar behandlas i RI-systemet. Brå får uppgifter om brott samt misstänkta och lagförda personer från polisen, ÅM, EBM och RI-systemet. KV får också uppgifter om domar via RI-systemet. Polisens system RAR och DurTvå

kommunicerar med Cåbra på så sätt att polisen kan skicka bland annat handlingar för beslut och förundersökningsprotokoll till Cåbra. Från Cåbra till DurTvå kan åklagaren skicka direktiv och beslut som polisen kan ta del av. RIF 7 myndigheterna, förutom polisen, har tillgång till uppgifter i folkbokföringsregistret via Navet. Polisen får idag folkbokföringsuppgifter via SPAR-registret[18] som innehåller fler uppgifter än bara folkbokföringsuppgifter. Det är SKV som ansvarar för folkbokföringsregistret.

Första etappen av RIF

Målet med den första etappen av RIF är att huvuddokumenten i brottmålsprocessen ska föras över elektroniskt i så kallad strukturerad form i rättskedjan. Den strukturerade formen innebär i detta sammanhang att vissa uppgifter får en bestämd form och placering i respektive system och när dessa uppgifter överförs så placeras de direkt i en bestämd form och plats även i mottagarens system. Innehåller uppgifterna exempelvis en adress så skickas den från polisens ”adressruta” i DurTvå eller Pust till ”adressrutan” i Cåbra. Strukturerad information kan exempelvis bestå av uppgifter om involverade personer eller uppgifter om brottet, men det kan också röra sig om administrativa uppgifter, såsom ärende- och målnummer. En del av uppgifter överförs i fritext, i PDF-format, och kallas i RIF-arbetet för ostrukturerat. Notera att begreppen strukturerat och ostrukturerat som används inom RIF inte överensstämmer med *PuL:s* motsvarande begrepp som beskrivs i avsnittet *Regler till skydd för den personliga integriteten* under rubriken om *personuppgiftslagen*.

Hösten 2012 ska följande moment vara genomförda av den första etappen

Strukturerad och ostrukturerad information enligt RIF:s definition skickas från Pust till Cåbra, såsom anmälan och förundersökningsprotokoll. Juridisk information utformad enligt kraven i RIF överförs från Cåbra, Pust och i viss mån från RAR till SOR. Cåbra kommunicerar även med MR i enlighet med kraven i RIF. RAR och DurTvå skickar uppgifter till Cåbra i enlighet med kraven i RIF. Stämningsansökan och förundersökningsprotokoll överförs elektroniskt från Cåbra till Vera strukturerat och ostrukturerat enligt RIF:s definition. Brottsanmälningar skickas

18 SKV håller f.n. på att avveckla det gamla SPAR-registret, vilket innebär att polisens tillgång till uppgifter från folkbokföringen inom kort kommer förändras.

strukturerat och ostrukturerat enligt RIF:s definition från SKV:s system BA till Cåbra.

Återstående del av den första etappen efter hösten 2012

RI-systemet ska börja fasas ut och domstolarna ska rapportera domar direkt till ÅM, EBM, KV, Brå och till BR. Juridisk information utformad enligt kraven i RIF ska överföras från Vera till SOR. SBE ska från BU skicka strukturerad och ostrukturerad information enligt RIF:s definition till Cåbra.

Den första etappen beräknas vara avslutad omkring halvårsskiftet 2013. Utfasningen av RI-systemet kommer emellertid inte vara klart förrän under 2014.

Andra etappen av RIF

Regeringen beslutade den 11 oktober 2012 att den andra etappen av RIF ska inledas parallellt med att den första etappen avslutas.[19] I den andra etappen ska det elektroniska informationsflödet utökas så att det omfattar flera arbetsprocesser och funktioner i brottmålsprocessen. Avsikten är att skapa förutsättningar för bättre statistikunderlag, tydligare styrning och bättre verksamhetsuppföljning. De nuvarande brottskoderna ska avvecklas. I myndigheternas uppdrag ingår det att skapa funktioner i arbetet som säkerställer integritetsskyddet. I etappen ska även Kustbevakningen och Tullverket ingå.

Överenskommelser om informationsutbyte

Inom RIF 7 har myndigheterna fattat överenskommelser med varandra om informationsutbyte. I överenskommelserna anges vilka parter som ingår överenskommelsen och syftet med det elektroniska utbytet. I överenskommelsen beskrivs informationsutbytet tekniskt. Det anges bland annat prestandakrav, teknisk uppföljning av utbytet och att kommunikationen ska följa Statskontorets standard för Spridnings- och Hämtningssystem (SHS). Överenskommelsen reglerar även ansvar för överföringen och kvaliteten i informationen, drift, felhantering, förvaltning och säkerhet. Beträffande säkerheten anges bland annat att informationsutbytet ska ske via det gemensamma kommunikationsnätet (SGSI), att parterna ansvarar för att kommunikationen intrångsskyddas av brandväggar och att spårbarhet och loggning ska ske enligt kraven

19 Regeringsbeslut 2012-10-11 Uppdrag att utveckla rättsväsendets informationsförsörjning Ju2012/6639/SI

som finns i dokumentet *Transportarkitektur för RIF (RIF0013)*. I överenskommelsen finns även krav på en årlig säkerhetsrevision. Alla de nämnda punkterna avser systemen ur teknisk hänseende och inte hur systemen används. Exempelvis avser spårbarhet och loggning hur systemen ska kunna identifiera att uppgifterna kommer från den myndighet som ska leverera informationen, att den leveransen sker på rätt sätt och att om det är några fel i leveransen att de kan härledas.

Några motsvarande överenskommelser eller skrivningar avseende den rättsliga aspekten finns inte. Inom RIF har en arbetsgrupp inrättats för gemensamma rättsliga frågor. Denna arbetsgrupp har träffats vid ett tillfälle sommaren 2012. Inom RIF är det de enskilda myndigheterna som ansvarar för att de överenskomna målen nås och det är de enskilda myndigheterna som ansvarar för att det arbete som sker överensstämmer med de regler som gäller för myndigheten.

Sekretessbrytande bestämmelser och elektroniskt utlämnande

Sekretessbrytande bestämmelser

Uppgifter som omfattas av sekretess får inte lämnas ut till enskilda eller till andra myndigheter om det inte finns ett undantag *i Offentlighets- och sekretesslagen (2009:400) (OSL)* eller i lag eller förordning som *OSL* hänvisar till *(8 kap. 1 § OSL).* Detsamma gäller mellan olika verksamhetsgrenar inom en myndighet om de är att betrakta som självständiga i förhållande till varandra *(8 kap. 2 § OSL)* som exempelvis de verksamheter inom SKV som sysslar med beskattning respektive brottsutredning.

De sekretessbrytande bestämmelserna återfinns huvudsakligen i *10 kap. OSL*. I kapitlet anges till exempel när uppgifter som rör misstankar om brott kan lämnas till polisen eller till åklagare utan hinder av sekretess *(10 kap. 19–24 §§ OSL)* och att uppgifter kan lämnas till en myndighet som ska ompröva en annan myndighets beslut eller åtgärd (*10 kap. 16 § OSL*). Rätt för den som är part i ett mål eller ärende att ta del av handlingarna, den så kallade *partsinsynen*, regleras i *10 kap 3 § OSL*.

I *10 kap. 2, 27 och 28 §§ OSL* finns också mer generella bestämmelser som tillåter en myndighet att lämna ut sekretessbelagda handlingar.

En myndighet kan med stöd av *10 kap. 2 § OSL* lämna ut en uppgift till en enskild eller till en annan myndighet om det är nödvändigt för att den utlämnande myndigheten ska kunna fullgöra sin verksamhet. Enligt de ursprungliga förarbetena till sekretesslagen ska bestämmelsen tillämpas restriktivt och sekretessen får bara efterges om det är en nödvändig förutsättning för att en myndighet ska kunna fullgöra ett åliggande som myndigheten har. Det är inte ett tillräckligt skäl att myndighetens arbete ska bli mer effektivt.[20] Notera också att det handlar om att den utlämnande myndigheten ska kunna utföra sitt uppdrag och inte om den mottagande myndighetens behov.

Generalklausulen i *10 kap. 27 § OSL* anger att sekretessen kan vika om det är uppenbart att intresset av att uppgiften lämnas har företräde framför det intresse som sekretessen ska skydda. Syftet med generalklausulen är att undvika oförutsedda hinder i myndigheternas verksamhet. Har det i lag eller förordning föreskrivits att uppgifter ”*bör*” eller ”*får*” lämnas är det en sådan situation där generalklausulen kan bli tillämplig om det inte finns andra sekretessbrytande bestämmelser. Generalklausulen kan också tillämpas vid rutinmässiga utbyten av uppgifter som inte är författningsreglerade. Bestämmelserna bygger emellertid på att rutinmässigt uppgiftsutbyte i regel ska vara författningsreglerat. I de undantagsfall när rutinmässigt uppgiftslämnande inte är författningsreglerat men likväl kan anses tillräckligt motiverat måste den intresseavvägning, som ska göras enligt generalklausulen, ske på förhand.[21] Bestämmelsen gäller, enligt dess *tredje stycke*, inte om utlämnandet strider mot lag eller förordning eller föreskrift som har meddelats med stöd av *PuL*.

Om en uppgiftsskyldighet följer av lag eller förordning hindrar inte sekretess att uppgifter lämnas till en annan myndighet enligt *10 kap. 28 § OSL*. Bestämmelsen gäller om det är föreskrivet att uppgiften ”*ska*” lämnas. Har en myndighet en föreskriven anmälningsplikt är det att betrakta som en sådan uppgiftsskyldighet. Anges det att uppgiften ”*får*” lämnas så är det istället generalklausulen i *27 §* som ska tillämpas. Om det enbart finns en allmän föreskrift om samarbete mellan myndigheterna gäller inte bestämmelsen.[22] I de särskilda registerförfattningarna återfinns bestämmelser om att uppgifter ska lämnas ut till andra myndigheter. För flera av RIF 7 myndigheterna framgår det av register-

20 Prop. 1979/80:2 Del. A s. 465 och 494
21 En kommentar på internet OSL 10:27
22 En kommentar på internet OSL 10:28

författningarna till exempel att de ska lämna de personuppgifter som är nödvändiga för att framställa rättsstatistik till den myndighet som ansvarar för att framställa sådan statistik. Den myndighet som avses är Brå enligt *förordningen (2001:100) om den officiella statistiken.* Det ingår således sekretessbrytande bestämmelser i registerförfattningarna.

Elektroniskt utlämnande

Finns det sekretessbrytande bestämmelser som anger att handlingen får lämnas ut trots att den är sekretessbelagd, så innebär det inte att handlingen kan lämnas ut i vilken form som helst. De regler som gäller för behandling av personuppgifter avgör om uppgifterna får lämnas ut i elektronisk form.

Det finns två uttryck som brukar användas för elektroniska utlämnanden och det är *direktåtkomst* och *utlämnande på medium för automatiserad behandling*. Det finns inte någon legaldefinition på begreppet direktåtkomst men den vedertagna innebörden är att någon utomstående direkt får tillgång att söka, sammanställa eller ta del av uppgifterna utan att kunna påverka innehållet. Dessutom innebär direktåtkomst att den utlämnande myndigheten inte har kontroll över vilka uppgifter mottagaren får del av. Åtkomsten kan däremot vara begränsad. Direktåtkomst används ibland även för att beskriva den interna åtkomsten till uppgifter inom en myndighet. För annat elektroniskt utlämnande än genom direktåtkomst används begreppet utlämnande på medium för automatiserad behandling. Det kan vara frågan om överföring via e-post, överföring via bärbara lagringsenheter eller direkt överföring från ett datorsystem till ett annat via ett kommunikationsnät.[23] [24]

I *PuL* anges det inte hur uppgifter får överlämnas eller göras tillgängliga utan istället ställs krav på att behandlingen ska vara tillräckligt säker i förhållande till hur integritetskänsliga uppgifterna som ska överföras är (*31 § PuL).* Det ställs även andra krav i *PuL* på utlämnande såsom att personuppgifter bara får lämnas ut om utlämnandet inte är oförenligt med de ändamål för vilka uppgifterna samlades in enligt *9 § första stycket punkten d PuL*, men då avses behandlingen i sig och inte formen.

I de särskilda registerförfattningarna regleras ibland vilka som har rätt till direktåtkomst eller utlämnande på medium för automatiserad behandling. I registerförfattningen kan det utläsas om regleringen är uttömmande eller inte. Nedan lämnas en redogörelse för de specifika

23 Prop.2011/12:45 s. 96

24 Direktåtkomst och utlämnande på medium för automatiserad behandling En rapport från E-delegationen

regler som gäller för myndigheterna inom RIF7 beträffande sekretessbrytande bestämmelser och elektroniskt utlämnande. Det anges även vilka sekretessbrytande bestämmelser som myndigheterna själva uppgett i enkätsvaren att de tillämpar.

RPS

Polisdatalagen reglerar uttömmande vad som gäller för elektroniskt utlämnande. Endast enstaka personuppgifter får lämnas ut på medium för automatiserad behandling om regeringen inte föreskrivit annat, *(2 kap. 20 polisdatalagen)* och utlämnande genom direktåtkomst är tillåtet bara i den utsträckning som följer av polisdatalagen, *(2 kap. 21 § polisdatalagen).*

Enligt *2 kap. 16 § polisdatalagen* har RPS, polismyndigheter, EBM, ÅM, Tullverket, Kustbevakningen och SKV rätt att ta del av personuppgifter som har gjorts gemensamt tillgängliga i polisens register, trots sekretess enligt *21 kap. 3 § första stycket och 35 kap. 1 § OSL*[25], om den mottagande myndigheten behöver uppgifterna i sin brottsbekämpande verksamhet. Enligt *3 kap. 8 § polisdatalagen* får dessa myndigheter ha direktåtkomst till uppgifterna. Om en myndighet medgetts direktåtkomst ställs det krav på myndigheten, att den ansvarar för att tillgången till personuppgifterna begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter. Av bestämmelsen framgår också att regeringen eller den myndighet som regeringen bestämmer kan meddela närmare föreskrifter om omfattningen av direktåtkomsten och om behörighet och säkerhet.

Enligt *17 § polisdataförordningen (2010:1155)* gäller begränsningen i *2 kap. 20 § polisdatalagen* inte för de myndigheter som enligt *3 kap. 8 § polisdatalagen* får ha direktåtkomst till uppgifterna. Det innebär att uppgifterna får lämnas ut även på medium för automatiserad behandling till de myndigheter som får ha direktåtkomst, om myndigheten behöver uppgifterna i sin brottsbekämpande verksamhet.

Regeringen har meddelat undantag från bestämmelsen i *2 kap. 20 § polisdatalagen* för ett antal aktörer, däribland Brå. Mer än enstaka personuppgifter får därför lämnas ut på medium för automatiserad behandling till Brå om uppgifterna är nödvändiga för att framställa

25 Sekretessen i 21 kap. 3 § första stycket OSL avser uppgifter om förföljda personers adress, telefon och liknande uppgifter och 35 kap. 1 § OSL avser sekretess till skydd för enskildas personliga och ekonomiska förhållanden i förundersökningar, brottsförebyggande verksamhet och register som används i brottsbekämpande verksamhet med mera

rättsstatistik enligt *2 kap. 14 § polisdatalagen* och *18 § polisdataförordningen*.

I enkätsvaret uppger RPS att de inte tillämpar några sekretessbrytande bestämmelser.

ÅM och EBM

I *17 § förordningen (2006:937) om behandling av personuppgifter inom åklagarväsendet* anges att utlämnande av uppgifter som är nödvändiga för att framställa rättsstatistik ska lämnas till den myndighet som ansvarar för att framställa sådan statistik, dvs. Brå. Några andra bestämmelser som anger vad som ska eller får lämnas ut finns inte. Enligt *4 §* förordningen är det bara anställda inom åklagarväsendet som har rätt till direktåtkomst till Cåbra. Utlämnande på medium för automatiserad behandling är inte reglerat i förordningen.

I betänkandet *Åklagarväsendets brottsbekämpning Integritet – Effektivitet (SOU 2008:87)* lämnas förslag på en ny registerförfattning för åklagarväsendet. Förslaget överensstämmer med bestämmelserna i den nya polisdatalagen. Det föreslås att RPS, polismyndigheter, EBM, ÅM, Tullverket, Kustbevakningen och SKV får möjlighet till direktåtkomst till gemensamt tillgängliga uppgifter. Endast enstaka personuppgifter får lämnas ut på medium för automatiserad behandling om regeringen inte meddelat föreskrifter eller i ett enskilt fall beslutat om att utlämnande för ske på sådant medium även i annat fall.

Som svar på om någon sekretessbrytandebestämmelse tillämpas hänvisar både ÅM och EBM till *10 kap. 28 § OSL,* att sekretess inte hindrar att uppgifter lämnas till en annan myndighet om uppgiftsskyldigheten följer av lag eller förordning.

DV

DV har som sekretessbrytande bestämmelse i OSL hänvisat till *10 kap. 2, 3, 16, 18, 27 och 28 §§ OSL*. DV har även nämnt följande.

Skyldighet för Sveriges domstolar att i vissa fall lämna uppgifter följer direkt av *5 § förordningen (1970:517) om rättsväsendets informationssystem* som föreskriver att uppgift om dom eller beslut av de allmänna domstolarna ska lämnas till RPS i de i förordningen angivna fallen. Av *26 § och 27 § förordningen om belastningsregister* följer att domstolen till RPS ska lämna uppgifter i fråga om den som på grund av beslut eller dom ska registreras i BR, detsamma gäller uppgifter som behövs för att gallra

i BR. För att uppgifterna i MR ska kunna gallras anges i *10 § förordningen om misstankeregistret* att domstolen till ÅM ska lämna uppgifter om dom eller beslut som vunnit laga kraft i den del som rör den utdömda påföljden eller avser sådan särskild rättsverkan av brott som innefattar betalningsskyldighet.

I *förordningen (2001:639) om registerföring m.m. vid allmänna domstolar med hjälp av automatiserad behandling* saknas bestämmelser om vilka former för utlämnande som tillåts. Eftersom förordningen gäller utöver *PuL* ska *PuL:s* bestämmelser tillämpas.

KV

I *9 § lagen (2001:617) om behandling av personuppgifter inom kriminalvården* anges att utlämnande ska ske av uppgifter som är nödvändiga för rättsstatistiken till den myndighet som ansvarar för att framställa denna, dvs. Brå. Det anges inte att det kan ske genom direktåtkomst eller genom utlämnande på medium för automatiserad behandling. I övrigt är det regeringen som enligt *10 §* kan föreskriva vilka myndigheter som personuppgifter ska lämnas ut till och om de får ha direktåtkomst till uppgifterna. Direktåtkomst ska vara förbehållen de personer vid myndigheten som på grund av sina arbetsuppgifter behöver tillgång till uppgifterna. Regeringen har i *37 § förordningen (2001:682) om behandling av personuppgifter inom kriminalvården* angett att uppgifter i det centrala kriminalvårdsregistret ska vid begäran lämnas ut till domstol, ÅM, EBM, RPS eller polismyndighet. RPS och polismyndigheterna ska också få ha direktåtkomst till registret.

KV anger i enkätsvaret att de inte tillämpar några sekretessbrytande bestämmelser utan skyldigheten att utlämna uppgifter framgår av förordningen.

SKV

SKV anger följande svar angående vilka sekretessbrytande bestämmelser som gäller för brottsanmälningar.

Uppgifter som ligger till grund för en brottsanmälan från beskattningsverksamheten omfattas av sekretess enligt *27 kap. OSL*. Av *10 kap. 28 § OSL* jämförd med *8 kap. 2 §* samma lag framgår att sekretess inte hindrar att uppgift lämnas till annan myndighet eller annan självständig verksamhetsgren inom samma myndighet om uppgiftsskyldighet följer av lag eller förordning. I *17 § skattebrottslagen (1971:69)* och *18 kap. 8 § skatteförfarandeförordningen (2011:1261)* finns bestämmelser om

anmälningsskyldighet för SKV. I svaret hänvisas också till *10 kap. 2 och 24, 27 §§ OSL*

Beträffande den brottsutredande verksamheten hänvisar SKV att som sekretessbrytandebestämmelser tillämpas *10 kap. 2 och 24 §§ OSL*. I *förordningen (2001:588) om behandling av uppgifter i Skatteverkets beskattningsverksamhet* finns reglerat utlämnande av uppgifter till andra myndigheter i *4–8 a §§*. I 5 a § i förordningen regleras SBE:s rätt att få ut uppgifter från beskattningsverksamheten.

I den utredande verksamheten som bedrivs av SBE ska uppgifter för rättsstatistik lämnas till Brå enligt *5 § lagen (1999:90) om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar*. I lagen bemyndigas regeringen att lämna föreskrifter om utlämnande i andra sammanhang. Uppgifter för rättsstatistiken lämnas idag inte direkt från SKV utan uppgifterna lämnas från Cåbra dvs. ÅM/EBM.

I *förordningen (1999:105) om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar* finns bara reglerat möjlighet till direktåtkomst och utlämnande till andra myndigheter beträffande underrättelseverksamheten *(7–10 §§)* och att uppgifter från en förundersökning i vissa fall kan utlämnas till konkursförvaltare *(10 a §)*.

Brå

Brå är i detta sammanhang endast mottagare av information.

Myndigheternas personuppgiftsansvar

Personuppgiftsansvarig är den som ensam eller tillsammans med andra bestämmer ändamålen med eller medlen för behandling av personuppgifter, enligt definitionen i *3 § PuL*. I registerförfattningarna anges det ofta vem som är personuppgiftsansvarig. Den som pekas ut som personuppgiftsansvarig i en registerförfattning stämmer för det mesta in i den definition som ges i *PuL*, men det är inte alltid så.

Inom RIF7 kan noteras att personuppgiftsansvaret hos polisen, DV och EBM avviker i förhållande till vad som anges i *3 § PuL*. Enligt *2 kap. 4 § polisdatalagen (2010:361)* är varje polismyndighet personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför. Det innebär att RPS utvecklar, förvaltar och lagrar uppgifter i RAR, DurTvå

och Pust, men det är polismyndigheterna som ensamma ansvarar för behandlingen. På samma sätt är en domstol enligt *1 § förordningen (2001:639) om registerföring m.m. vid allmänna domstolar med hjälp av automatiserad behandling* personuppgiftsansvarig för den behandling av personuppgifter som domstolen utför, men det är DV som utvecklar, lagrar uppgifter och också delvis förvaltar Vera.

RPS är även personuppgiftsansvarig för den behandling av personuppgifter som utförs i polisens verksamhet vid EBM enligt *1 kap. 4 § polisdatalagen*. Vad som avses med polisens verksamhet vid EBM är emellertid inte helt klart. Enligt den ursprungliga tanken var EBM ansvarig för den polisverksamhet som var en del av myndighetens samlade verksamhet och EBM omfattades inte av den gamla polisdatalagen eftersom EBM är en åklagarmyndighet. För att EBM skulle kunna bedriva kriminalunderrättelseverksamhet ändrades den gamla *polisdatalagen (1998:622)* och gjordes tillämplig på EBM från den 1 januari 2004 med följande motivering.

> *... att bedriva kriminalunderrättelseverksamhet är emellertid, och bör framdeles vara, en rent polisiär uppgift. Den mest lämpliga lösningen är därför att utvidga polisdatalagens tillämpningsområde till att omfatta polisverksamhet vid Ekobrottsmyndigheten. En sådan ordning bör kunna genomföras utan att utvecklingen av det integrerade arbetssättet inom myndigheten hindras, eftersom den aktuella verksamheten inte kräver samverkan mellan polis och åklagare på sätt som gäller för övrig verksamhet inom myndigheten. Mot bakgrund av det anförda anser regeringen därför att polisdatalagen skall omfatta polisverksamhet även vid Ekobrottsmyndigheten.*[26]

I förarbetena till den nya polisdatalagen anges att någon förändring beträffande personuppgiftsansvaret vid EBM inte är motiverad. Samtidigt uppges det att skiljelinjen för ansvaret går mellan de polisiära datasystemen och åklagarväsendets datasystem.[27] De så kallade polisiära datasystemen används inom EBM för långt mer än enbart kriminalunderrättelseverksamhet, eftersom RAR och DurTvå används i EBM:s utredningsverksamhet. Vad som numera ska förstås med polisens verksamhet vid EBM måste därför bedömas som oklart.

EBM har också en oklar gräns mot ÅM. EBM använder Cåbra för sin ärendehantering, men det är ÅM som utvecklar, förvaltar och lagrar uppgifter. Något personbiträdesavtal finns inte mellan EBM och ÅM.

26 Prop. 2002/03:144 s. 16-17 Övergångsbestämmelserna i polisdatalagen m.m.
27 Prop. 2009/10:85 s. 93 Integritet och effektivitet i polisens brottsbekämpande verksamhet

Riktiga uppgifter och korrekt behandling

Enligt *9 § första stycket g och h PuL* är det ett grundläggande krav vid behandling av personuppgifter att de uppgifter som behandlas är riktiga och om det är nödvändigt, att de är aktuella och att alla rimliga åtgärder vidtas för att rätta, blockera eller utplåna sådana personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålen med behandlingen.

Förutom att personuppgifterna ska vara riktiga, ska behandlingen ske på ett korrekt sätt och i enlighet med god sed, enligt *9 § första stycket b PuL*.

Justitiekanslern (JK) beslutade nyligen att staten skulle betala skadestånd till en person, för att en tingsrätt behandlat personuppgifter om honom i strid mot bestämmelser i *PuL* om att uppgifterna ska vara riktiga och behandlingen ska vara korrekt. Tingsrätten hade på sin digitala uppropslista anslagit att häktningsförhandling skulle hållas beträffande fyra ungdomar, trots att häktningsförhandling bara skulle hållas gentemot tre av ungdomarna. Orsaken till att även den fjärde ungdomen var med på uppropslistan var att åklagaren tidigare inkommit med begäran om offentlig försvarare för alla fyra såsom misstänkta för brott. Förundersökningen gentemot den fjärde ungdomen lades ned dagen efter häktningsförhandlingen. JK ansåg att uppgiften i uppropslistan inte var riktig eller aktuell i *PuL:*s mening och att behandlingen av personuppgifterna inte heller kunde anses ha skett på ett korrekt sätt och i enlighet med god sed, JK beslutade därför att staten skulle betala skadestånd enligt *48 § PuL*. I beslutet noteras också att JK vid en underhandskontakt med Domstolsverket har fått uppgift om att det är tekniskt möjligt att redigera innehållet i de uppropslistor som anslås på domstolarnas informationstavlor. Domstolsverket har dock inte kunnat ange i vilken utsträckning domstolarna tillämpar denna möjlighet. [28]
JK har i ett annat ärende gällande skadeståndsanspråk mot staten beslutat att tillerkänna skadestånd till en person för att polisen inte angett aktuella uppgifter när förundersökningen i ärendet redovisades till åklagaren. Polisen hade vid redovisningen inte uppmärksammat att personen ifråga, under utredningstiden, erhållit så kallad sekretessmarkering genom ett beslut av SKV. De sekretessmarkerade adressuppgifterna blev offentliga hos tingsrätten i samband med att rätten förordnande målsägandebiträde. [29]

28 Justitiekanslern beslut den 24 september 2012 i ärende dnr 6461-11-42
29 Justitiekanslerns beslut den 25 juni 2012 i ärende dnr 1350-11-40

Huvudregeln inom RIF är att var och en av myndigheterna ansvarar för att uppgifterna är riktiga i sina respektive system. Någon möjlighet att säkerställa att uppgifter rättas samtidigt i alla led finns inte. Det finns en överenskommelse mellan myndigheterna att uppgifter ska kontrolleras mot folkbokföringen innan de förs vidare i rättskedjan. I övrigt har det i RIF förts diskussioner om rättelse av beslut och domar. I oktober 2010 beslutades av RIF-gruppen att man skulle se hur materiella fel i uppgifterna ska hanteras, framförallt när det gäller domar och beslut. Det benämndes *utbytesrelaterad registervård*. Uppdraget är fortfarande under beredning hos RIF-gruppen.

Behörighet och spårbarhet

Det är totalt över 55 000 anställda inom de aktuella myndigheterna inom RIF7. För RPS del räknas hela polisväsendet och beträffande DV bara de allmänna domstolarna. Behörighet till något av de aktuella systemen har sammanlagt cirka 45 000 personer.[30] Hur stor tillgång till uppgifter i systemen de behöriga har skiljer sig åt från myndighet till myndighet.

I *31 § PuL* anges det att den personuppgiftsansvarige ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. En del av säkerhetsåtgärderna utgörs av kontroll av behörigheter och loggning. Dessutom innehåller de grundläggande kraven på behandling av personuppgifter i *9 § PuL* restriktioner vid behandling av personuppgifter som också påverkar behörigheterna. Det är framförallt *punkterna c, d och f* som är av intresse i detta sammanhang – att personuppgifter bara får samlas in för särskilt angivna ändamål, att uppgifterna inte får behandlas på något sätt som är oförenligt med de ändamål som de samlats in för och att inte fler personuppgifter behandlas än vad som är nödvändigt med hänsyn till ändamålen.

RPS

Enligt *2 kap. 11 § polisdatalagen* ska tillgången till personuppgifterna begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter. Varje polismyndighet ansvarar för att det inom den egna myndigheten finns rutiner för tilldelning, förändring, borttagning och regelbunden uppföljning av behörigheter för åtkomst till personuppgifter, *3 § polisdataförordningen (2010:1155)*.

30 MR och BR är inte medräknade

I *9 kap. Rikspolisstyrelsens föreskrifter om säkerhet vid Polisens informationsbehandling med stöd av IT (RPSFS 2009:4 FAP 174-1)* anges att behörighet till polisens IT-system förutsätter att personen bedöms vara lämplig ur säkerhetssynpunkt, har erforderliga kunskaper för att använda IT-systemet och har behov av uppgifterna i systemet för att kunna fullgöra sina arbetsuppgifter. Det är polismyndigheterna som beslutar om behörighet. Användaren visar sin behörighet genom både behörighetskort och lösenord. I IT-system som är avsedda för behandling av särskilt skyddsvärda uppgifter ska varje åtkomst och aktivitet i systemet loggas. Användaraktiviteter som kan tolkas som försök till intrång eller brott mot behörighetsregler ska registreras i logg samt ska kunna generera larm. I övriga IT-system ska loggning ske i den utsträckning som myndighetens verksamhet kräver det. För de IT-system där loggning används ska loggningens funktion övervakas och loggen ska bevaras i minst fem år. Myndigheten ska se till att loggar följs upp och vid behov analyseras.

RAR har cirka 25 000 användare. Användare är både poliser och civilanställda som arbetar hos polisen. DurTvå har också cirka 25 000 användare som är poliser, civila utredare, assistenter eller arkivarier. Pust har cirka 27 000 användare i kategorierna utredare, förundersökningsledare och arkivarie. I RAR, DurTvå och Pust loggas alla åtgärder även sökningar . Användarna informeras om att loggning sker i samband med inloggning och genom den ovan angivna föreskriften om säkerhet vid Polisens informationsbehandling med stöd av IT.

I *lagen (1998:621) om misstankeregister* och *förordningen (1999:1135) om misstankeregister* anges vilka som får ha tillgång till eller få uppgifter ur MR. När det gäller BR regleras tillgången till uppgifterna i *lagen (1998:620) om belastningsregister* eller *förordningen (1999: 1134) om belastningsregister.* Det rör sig om ett stort antal svenska myndigheter som har rätt att få del av uppgifterna, men också enskilda och utländska myndigheter har i viss mån rätt att få del av uppgifter från MR och BR. Direktåtkomst till MR har polismyndigheter, SKV, Tullverket, Kustbevakningen, ÅM, EBM, KV, Migrationsverket och i vissa delar Transportstyrelsen och länsstyrelserna, enligt *6 och 7 §§ förordningen (1999:1135) om misstankeregister.* Rätten till direktåtkomst till BR regleras i *19 och 20 §§ förordningen (1999:1134) om belastningsregister.* Direktåtkomst till BR har polismyndigheter, SKV, Tullverket, Kustbevakningen, ÅM, EBM, KV, Migrationsverket och allmänna domstolar. Transportstyrelsen, länsstyrelserna och Socialstyrelsen får ha direktåtkomst till BR i vissa delar. De myndigheter utanför polisväsendet som har tillgång till MR och BR

registreras bara som en användare hos RPS, oavsett hur många det är inom myndigheten som har tillgång till systemen. RPS har därför inte kännedom om hur många slutanvändare det faktiskt är frågan om, men uppskattar att MR och BR vardera har cirka 60 000 slutanvändare. Inom polisens nätverk loggas alla åtgärder. RPS har överenskommelser med de myndigheter som får har direktåtkomst till MR och BR som omfattar frågor om behörighet, loggning och säkerhet.

RAR, DurTvå, Pust, MR och BR omfattas av polisens Centrala Säkerhetslogg (CSL)som analyserar användningen av personuppgifter och aktivt söker tecken på otillåten eller obehörig åtkomst.

Allmänheten har inte tillgång till Pust, RAR eller DurTvå. Till systemen finns det en funktion som kallas *"Allmänhetens register"*, men den funktionen är inte i bruk på grund av tekniska hinder. Enligt RPS visas inte i registret några personuppgifter.

ÅM

I *förordningen (2006:937) om behandling av personuppgifter inom åklagarväsendet* anges det att det inom åklagarväsendet får finnas en samling uppgifter och handlingar som med hjälp av automatiserad behandling används gemensamt i åklagarverksamheten vid ÅM och EBM. Direktåtkomst till uppgifter och handlingar i åklagarverksamheten ska begränsas till vad en åklagare eller annan anställd vid ÅM eller EBM behöver för att på ett ändamålsenligt sätt kunna utföra sina arbetsuppgifter och till handlingar som förekommer i ett ärende hos den egna myndigheten.

Till Cåbra har enligt ÅM 1 600 åklagare och administratörer behörighet. Dessa arbetar inom myndigheten och EBM. Behörighetsprofilerna i Cåbra är administratör, åklagare, kammarchef och systemadministratör. Enligt *Åklagarmyndighetens föreskrifter om IT-säkerhet inom åklagarväsendet (ÅFS 2006:1)* är det myndighetschefen som beslutar om behörighet, ändring och upphörande av behörighet, men med möjlighet att delegera det till chef för åklagarkammare och enhetschef.

Loggning sker av utförda åtgärder och åtkomst. Användarna informeras om att loggning sker. Någon systematisk logguppföljning sker inte. ÅM har inte några särskilda rutiner för att informera användarna om vilka begränsningar som föreligger utan det framgår av den aktuella förordningen.

För allmänheten finns som regel en *”Allmänhetens dator”* på åklagarkamrarna. Ärendenumren och rena diarieuppgifter syns på allmänhetens dator. Någon direktåtkomst i övrigt finns inte till Cåbra.

ÅM har i *Åklagarmyndighetens föreskrifter om skyldighet att i vissa fall skydda innehållet i ärenden och dokument från direktåtkomst i verksamhetsstödet Cåbra (ÅFS 2007:3)* föreskrivit att dokument och ärenden i Cåbra ska ges åtkomstskydd endast när det finns skäl för det enligt vad som framgår av föreskriften och inte göras mer omfattande än vad som är nödvändigt i varje enskilt fall. De situationer där åtkomstskydd kan användas är om det rör någon anställd inom åklagarväsendet eller polisen eller en närstående till en sådan person, om det rör en medialt uppmärksammad person eller om det finns risk för att brott kommer begås mot personer som har anknytning till ärendet exempelvis bevispersoner. Åtkomstskydd kan även användas för uppgifter som är särskilt känsliga ur utredningssynpunkt. Dessutom kan åtkomstskydd ges om det är uppenbart att det behövs. Uppgifter som inte är åtkomstskyddade kan läsas av alla som har behörighet till Cåbra.

EBM

Det som beskrivits angående ÅM gäller även för EBM beträffande behörighet och spårbarhet. Inom EBM är det endast anställda som har behörighet till Cåbra, sammanlagt strax under 200 personer. De poliser som arbetar på EBM är, som tidigare beskrivits, inte anställda på EBM och de har därför inte behörighet till Cåbra.[31]

DV

Vera innehåller funktionalitet för att tilldela användarna olika behörigheter såsom central- och lokal systemadministratör, registrator, personal i dömande verksamhet, övrig personal och allmänhet. Behörigheterna är styrande för vilka åtgärder en användare kan vidta i systemet och vilken registrerade uppgifter som användaren kan ta del av. Behörigheterna är begränsade till den domstol till vilken användaren är knuten förutom vad gäller den centrala systemadministratörsbehörigheten.

Personal vid DV kan tilldelas central systembehörighet efter godkännande av närmaste chef och beslut av produktansvarig för Vera. Domstolarna beslutar och administrerar övriga användares behörigheter. Exakt hur många användare av Vera det finns vid domstolarna saknar därför DV kännedom om. DV uppger emellertid att det kan antas att

31 4 § förordningen (2006:937) om behandling av personuppgifter inom åklagarväsendet

i princip samtliga anställda vid Sveriges domstolar har någon form av behörighet i Vera, vilket innebär något över 6 000 användare. DV har inte meddelat någon föreskrift om behörighetsbegränsningar, utan endast en generell föreskrift *Domstolsverkets föreskrifter om informationssäkerhet för gemensamma IT-system (DVFS 2012:1)*. Det är respektive domstol som har ansvar för att informera användarna om vilka krav och begränsningar som föreligger.

Någon generell loggning av vilka åtgärder som en användare vidtar i Vera finns inte, utan loggning sker vid raderingar eller ändringar av vissa särskilt angivna uppgifter och när någon tagit del av vissa typer av uppgifter. Det är de enskilda domstolarna som har ansvaret för uppföljning av de loggar som förs. Om domstolarna har särskilda rutiner för och i vilken utsträckning de genomför uppföljning av loggar saknar DV kännedom om.

I de fall loggning sker vid en åtgärd eller när någon tar del av en uppgift varnar Vera att loggning kommer att ske. DV genomför också centrala utbildningar för personal, så kallade lokala *Veralärare*, som finns ute vid domstolarna och som har till uppgift att utbilda personalen vid domstolarna i frågor kring verksamhetsstödet Vera. Vid de centrala utbildningarna lämnas bland annat information kring de loggningsfunktioner som finns i Vera. Viss information kring den loggning som sker finns även publicerad på Sveriges Domstolars intranät *Doris*.

Inga andra myndigheter inom RIF7 har direktåtkomst till systemet, men däremot har de allmänna domstolarna sinsemellan möjlighet att under vissa förutsättningar ta del av uppgifter som har registrerats hos andra domstolsinstanser. Efter att ett mål har överklagats bereds överrätten tillgång till samtliga aktörsuppgifter, dagboksblad samt upprättade och inskannade dokument i underrättens mål i Vera. Underrätten bereds tillgång till motsvarande uppgifter hos överrätten med undantag för uppgifter som är sekretessmarkerade. Denna integration gäller mellan samtliga instanser. Uppgifterna blir automatiskt tillgänglig mellan domstolarna i och med att registrator vid aktuell överrätt registrerar det nya målet vid ett överklagande.

Vid de enskilda domstolarna finns det för allmänheten terminaler som möjliggör sökningar i verksamhetsregistret vid den domstol där terminalen är belägen. I allmänhetens terminal visas uppgifter såsom målnummer, vad saken rör dvs. brottsrubricering och lagrum, aktörer, uppgifter om dom och beslut. Aktörer är de personer som är inblandade i processen såsom misstänkt, målsäganden, vittnen men också försvarare

och åklagare. Misstänkt och målsäganden finns redovisade med både namn och personnummer. I ett mål kan det som antecknats i diariet läsas. Det är möjligt att söka i systemet på olika sätt. Det går att söka dels direkt efter ett specifikt mål utifrån exempelvis målnumret. Det går också att söka efter en person utifrån namn eller personnummer. Det är också möjligt att söka efter samtliga mål tillhörande viss brottsgrupp såsom exempelvis ”Brott mot person”. Även avslutade brott är sökbara.

När Datainspektionen gjorde sökningar på *Allmänhetens terminal* vid Stockholms tingsrätt i oktober 2012, påträffades ett mål avseende grovt skattebrott och grovt bokföringsbrott som inkom 2006-09-13 med en begäran om offentlig försvarare och avslutades 2007-10-16, genom att det avskrevs efter att en skrivelse och beslut inkommit från EBM. Misstänkts namn och personnummer angavs. Vid en slagning på personnumret på den misstänkte kunde konstateras att den registrerade även förekom i ett konkursmål som inleddes 2005-10-11 och ett civilmål, en gemensam ansökan om äktenskapsskillnad 2006-08-11, dessa överfördes till en annan tingsrätt 2007. Ett annat mål som påträffades avsåg grov kvinnofridskränkning. Det avslutades 2012-02-10 efter att åklagare på City Åklagarkammare lagt ned förundersökningen. Misstänkt och målsäganden angavs med namn och personnummer i målet. Vid en sökning på målsägandens personnummer påträffades ett tvistemål (FT) som avslutades 2006-02-27. En sökning skedde också på mål som inkommit den aktuella dagen som sökningarna gjordes. I den sökningen erhölls bland annat träff på ett mål rörande våldtäkt. Det som var antecknat i målet var att en framställan om målsägandebiträde hade inkommit till tingsrätten under dagen. Målsägandens namn och personnummer angavs.

KV

Direktåtkomst till de personuppgifter som behandlas enligt *lagen (2001:617) om behandling av personuppgifter inom kriminalvården* ska enligt lagens *6 §* vara förbehållen de personer som på grund av sina arbetsuppgifter inom KV behöver tillgång till uppgifterna.

Behörighet att använda KVR har alla inom KV med klientkontakt vilket innebär cirka 10 000 personer. Behörigheten tilldelas av verksamhetsområdeschefen inom sitt område. Huvudkontoret beslutar om landsomfattande behörighet. Behörigheten är anpassad efter vad användaren behöver för sin arbetsuppgift. KV ger information om de krav- och begränsningar som föreligger till alla nyanställda genom ”*Information om sekretess och användning av Kriminalvårdens datorer*”. I den lämnas också

information om att alla transaktioner loggas. KV gör både slumpmässiga uppföljningar och mer riktade kontroller av loggen.

Enligt *förordningen (2001:682) om behandling av personuppgifter inom kriminalvården* får Regeringskansliet, RPS och polismyndigheter ha direktåtkomst till Centrala kriminalregistret (KVR).

SKV

All personal i operativ verksamhet inom beskattning, brottsbekämpning och kontroll kan vara aktuella som anmälare i systemet BA och teoretiskt kan det därför bli frågan om cirka 4 000 användare. I praktiken uppskattar SKV att antalet användare i systemet kommer att vara cirka 2 000 personer plus närmare 300 användare i kategorierna kvalitetssäkrare, beslutande, regionsamordnare och administratörer.

I BU ska det enligt planen finnas fyra olika rollerna – chef, SBE-samordnare, brottsutredare och administratör. Varje roll ska ges en behörighet utifrån vad den rollen behöver enligt en behörighetsstruktur. Behörigheterna beställs av närmaste chef och tilldelas centralt av behörighetsfunktionen. Totalt kommer det att vara cirka 250 användare i systemet varav cirka 200 är brottsutredare.

I systemen skrivs en auditlogg; vem som skapat, uppdaterat, tagit bort eller läst information i systemet. Auditloggen övervakas kontinuerligt. SKV har en centraliserad övervakning. Loggen ger möjligheten att spåra vad en användare har gjort i systemet. All användning av SKV:s informationssystem följs upp enligt *Skatteverkets riktlinjer för användning av logguppgifter* (*dnr: 131 213193-07/111).* Information om detta finns på SKV:s intranät, som är åtkomligt för samtliga anställda. I *Riktlinjer om användning av Skatteverkets arbetsredskap (dnr 778223-09/111)* anges att all användning av IT-systemen följs upp. Information ges även vid utbildning till exempel av nyanställda.

Andra myndigheter kommer inte ha direktåtkomst till systemen. Inte heller allmänheten kommer att ha tillgång till systemen.

Brå

Behörighet till systemet har sammanlagt 24 personer på Brå. Det är personer som sysslar med rättsstatistik eller med IT. Behörigheten tilldelas av närmaste enhetschef. I samband därmed ger enhetschefen muntligen information om de krav och begränsningar som föreligger. En jurist från Brå:s juridiska sekretariat har dessutom, med varje enskild

anställd, en genomgång av innebörden av tillämpliga sekretessbestämmelser och av de krav *PuL* ställer på personuppgiftsbehandling. Därutöver går personal från IT-enheten igenom IT-säkerhet med nyanställda.

Alla förändringar som sker i systemet loggas. Vilket också användarna informeras om. Någon systematisk logguppföljning sker inte.

Vare sig allmänheten eller andra myndigheter har tillgång till uppgifter i systemet. Däremot kan alla ta del av den statistik som Brå producerar med stöd av uppgifterna i SOR. Statistiken publiceras på Brå:s webbsida och innehåller inte några personuppgifter.

Känsliga personuppgifter

Känsliga personuppgifter är enligt *13 § PuL* uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförbund och uppgifter som rör hälsa eller sexualliv. Det är enligt nämnda paragraf förbjudet att behandla känsliga personuppgifter. Från detta förbud finns det ett antal undantag i *PuL*. Finns det samtycke från den registrerade så får till exempel behandling ske enligt *15 § PuL*. Behandling som är nödvändig för att rättsliga anspråk ska kunna fastställas, göras gällande eller försvaras får också ske enligt *16 § första stycket punkten c.* Av intresse i detta sammanhang kan också undantaget i *19 §* vara som anger att känsliga personuppgifter får behandlas för forsknings- och statistikändamål i vissa beskrivna situationer. Det finns i *20 §* ett bemyndigande för regeringen eller den myndighet som regeringen bestämmer att meddela föreskrifter om ytterligare undantag från förbudet i *13 §,* om det behövs med hänsyn till ett viktigt allmänt intresse. I *8 § personuppgiftsförordningen (1998:1191)* anges att utöver vad som följer av undantaget i *PuL* får känsliga personuppgifter behandlas av en myndighet i löpande text om uppgifterna har lämnats i ett ärende eller är nödvändigt för handläggningen av det. I många registerförfattningar finns särskilda regler som avser behandling av känsliga personuppgifter.

RPS

Enligt *2 kap. 9–10 §§ polisdatalagen* får uppgifter om en person inte behandlas enbart på grund av vad som är känt om personens ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse,

medlemskap i fackförening, hälsa eller sexualliv. Om uppgifter om en person behandlas på annan grund får de kompletteras med sådana uppgifter som avses i första stycket när det är absolut nödvändigt för syftet med behandlingen. Uppgifter får också behandlas om det är nödvändigt för diarieföring eller om uppgifterna har lämnats till polisen i en anmälan eller liknande och behandlingen är nödvändig för handläggningen. I *3 kap. 5 § första stycket polisdatalagen* anges att avseende gemensamt tillgängliga uppgifter får inte känsliga personuppgifter användas som sökbegrepp.

RPS uppger beträffande såväl RAR, DurTvå som Pust att känsliga personuppgifter endast överförs och behandlas i ostrukturerad form.

ÅM och EBM

För åklagarväsendet regleras behandlingen av känsliga personuppgifter i *10 § förordningen (2006:937) om behandling av personuppgifter inom åklagarväsendet* och begränsningen gällande att använda känsliga personuppgifter som sökbegrepp återfinns i *14 §* i förordningen. Bestämmelserna överensstämmer väl med vad som gäller för polisen enligt polisdatalagen.

ÅM och EBM uppger att de i brottmålsprocessen inte hanterar känsliga personuppgifter strukturerat. Känsliga personuppgifter kan dock enligt ÅM och EBM förekomma i underliggande handlingar i ett ärende. Om en handling omfattas av sekretess enligt *5 kap. 1 § OSL* ska den enligt ÅM:s ärendehanteringshandbok sekretesskyddas vid registreringen.

DV

I *förordningen (2001:639) om registerföring m.m. vid allmänna domstolar med hjälp av automatiserad behandling* återfinns bestämmelserna om känsliga personuppgifter i *3 § andra stycket, 4 § första stycket*. De allmänna domstolarnas bestämmelser liknar polisens och åklagarväsendets bestämmelser, men i bestämmelserna för de allmänna domstolarna anges att restriktioner även finns för att behandla uppgifter om lagöverträdelser enligt *21 § PuL*.

DV anger att känsliga personuppgifter inte registreras i strukturerad form i verksamhetsregistret. I verksamhetsregistret kan det inte utläsas om ett dokument eller en ljud- eller bildupptagning kan tänkas innehålla känsliga personuppgifter. Någon särskild kommunikationslösning vid överföring av sådant som kan tänkas innehålla känsliga personuppgifter finns inte. I de fall de känsliga uppgifterna är sekretessmarkerade

framgår det emellertid av Vera och sekretessbelagda uppgifter förs inte heller över från överrätt till underrätt.

KV

Enligt *5 § lagen (2001:617) om behandling av personuppgifter inom kriminalvården* får känsliga personuppgifterna behandlas om de kompletterar andra personuppgifter som behandlas på annan grund och att det är absolut nödvändigt för syftet med behandlingen. När det gäller möjligheten att använda känsliga personuppgifter som sökbegrepp så är det möjligt för KV om regeringen föreskriver det och det är i syfte att upprätthålla säkerheten och förebygga brott under den tid som personen är föremål för KV:s insatser. Beträffande personutredningar gäller inte dessa begränsningar.

KV har på frågan om de behandlar känsliga personuppgifter, vilken typ av uppgifter det är och i så fall i vilket sammanhang de känsliga personuppgifterna behandlas, hänvisat till att det framgår av *lagen (2001:617) om behandling av personuppgifter inom kriminalvården* och *förordningen (2001:682) om behandling av personuppgifter inom kriminalvården*. Några känsliga personuppgifter överförs inte enligt KV.

SKV

Beskattningsverksamheten är av mindre intresse i detta sammanhang och berörs därför inte.

I *4 § lagen (1997: 1024) om Skatteverkets medverkan i brottsutredningar* anges att känsliga personuppgifter endast får behandlas om de kompletterar andra personuppgifter som behandlas på annan grund och det ska också vara oundgängligen nödvändigt för syftet med behandlingen. Till skillnad från vad som gäller för de andra myndigheterna anger lagen inte någon sökbegränsning beträffande känsliga personuppgifter.

Enligt SKV behandlas inte känsliga personuppgifter som strukturerad information. Känsliga personuppgifter kan komma att behandlas om uppgifterna finns eller tas in i handlingar som upprättas i eller bifogas ärendet. Det är då oftast fråga om uppgifter som lämnats av den registrerade själv, till exempel vid förhör eller som en upplysning i en deklaration, och som bedöms nödvändiga för handläggning av ärendet. Den ansvarige tjänstemannen prövar om en handling med känsliga uppgifter ska tas med i samband med handläggning av ärendet.

Brå

Av *15 § lagen (2001:99) om den officiella statistiken* framgår att behandling av känsliga personuppgifter *enligt 13 § PuL* och uppgifter om lagöverträdelser med mera enligt *21 § PuL,* endast får ske om det är tillåtet enligt föreskrift som regeringen meddelar. I en bilaga till *förordningen (2001:100) om den officiella statistiken* har regeringen meddelat att Brå får behandla båda dessa kategorier av personuppgifter i den mån de avser brott, domar i brottmål och straffprocessuella tvångsmedel.

Brå uppger att de hanterar känsliga personuppgifter. Det kan dels röra sig om uppgifter som avslöjar ras eller etniskt ursprung, dels uppgifter som rör hälsa och sexualliv. Avseende uppgifter som rör hälsa kan det till exempel vara uppgifter om psykisk hälsa som har betydelse för domslutet eller uppgifter om narkotikamissbruk. Brå har vidare gjort bedömningen att personuppgifter som rör sexualbrott ska anses vara uppgifter som rör sexualliv. Känsliga personuppgifter beaktas inte på något särskilt sätt hos Brå. Samma höga skyddsnivå tillämpas för samtliga uppgifter som inkommer till Brå. Samtliga uppgifter omfattas av stark sekretess.

Bevarande av uppgifter

Ett grundläggande krav på behandlingen av personuppgifter är, enligt *9 § första stycket punkten f PuL*, att de inte bevaras längre än nödvändigt med hänsyn till ändamålet med behandlingen. I offentlig verksamhet finns emellertid ett krav att arkivera och bevara allmänna handlingar som uttryckligen har företräde framför *PuL,* enligt *8 § andra stycket PuL*. Kravet på att bevara uppgifter innebär inte att uppgifterna får behandlas i den löpande verksamheten obegränsad tid. Många registerförfattningar anger hur länge uppgifter får behandlas i verksamheten.

RPS

I polisdatalagen anges att uppgifter som förekommer i ärenden – om utredning eller beivrande av brott och som gjorts gemensamt tillgängliga – inte ska gallras. Däremot finns det begränsningar för hur länge uppgifterna får användas i polisens brottsbekämpande verksamhet i *3 kap. 9–13 §§ polisdatalagen*. I *13 §* anges exempelvis att en person inte får vara sökbar som misstänkt om en förundersökning eller ett åtal har lagts ned eller en frikännande dom, som har vunnit laga kraft, har meddelats. Regeringen har möjlighet att besluta om undantag från bestämmelserna

som begränsar behandlingen av uppgifter. Så har också skett i *20–26 §§ polisdataförordningen,* där exempelvis undantag finns för sökningar som sker för att det finns anledning att återuppta en förundersökning eller för att det av särskilda skäl är nödvändigt för att finna samband mellan brott eller för att förebygga och förhindra återfall.

Enligt övergångsbestämmelserna till polisdatalagen behöver inte sökbegränsningarna tillämpas förrän den 1 januari 2015. Det beror på att kraven inte kan uppfyllas utan att det vidtas åtgärder i systemen. Polisen behöver bland annat få återkoppling från domstolarna om exempelvis frikännande dom för att veta att personen inte längre ska vara sökbar. Förväntningarna är att det arbete som sker inom RIF ska leda till att kraven i *polisdatalagen* ska kunna uppfyllas, vilket i förarbetena uttrycktes enligt följande.

> *Vid övrig behandling av personuppgifter är det framför allt några bestämmelser i den nya lagen som polisen kan få svårigheter att tillämpa redan vid ikraftträdandet. Detta bekräftas i huvudsak av Rikspolisstyrelsen i redovisningen av uppdraget. Det rör sig om delar av regleringen angående gemensamt tillgängliga uppgifter, nämligen vissa av bestämmelserna om särskilda upplysningar, sökbegränsningar samt om behandling av uppgifter i brottsanmälningar och avslutade förundersökningar.*
>
> *Gemensamt för dessa bestämmelser är att de förutsätter en återkoppling till polisen från åklagarväsendet när en åklagarledd förundersökning eller ett åtal har lagts ned och från domstol om lagakraftvunna domar. Som Rikspolisstyrelsen påtalar saknas det för närvarande sådana rutiner för återkoppling. Det behövs därför övergångsbestämmelser som under en tid medger undantag från tillämpningen av de aktuella bestämmelserna. Rådet för rättsväsendets informationsförsörjning bedriver arbete som bl.a. syftar till att åstadkomma en rutin för elektronisk återkoppling till polisen av beslut av myndigheter i senare led i rättskedjan. Åklagarmyndigheten och Ekobrottsmyndigheten framhåller vikten av att ikraftträdande- och övergångsbestämmelserna utformas med beaktande av det arbete som pågår.*
>
> *I fråga om bestämmelserna om sökning är det inte enbart bristen på återkoppling som motiverar övergångsbestämmelser. Bestämmelserna om sökbegränsningar har ingen motsvarighet i gällande reglering och*

det är enligt Rikspolisstyrelsen svårt att hinna åstadkomma nödvändiga anpassningar av nuvarande system före lagens ikraftträdande.[32]

Av *13 § lagen (1998:621) om misstankeregister* följer att en uppgift om misstanke om brott ska gallras ur MR om en förundersökning eller ett åtal läggs ned eller om det avkunnats en dom som vunnit laga kraft eller om ett strafföreläggande godkänts.

I BR gallras uppgifterna enligt bestämmelser i *16–18 §§ lagen (1998:620) om belastningsregister.* En uppgift ska gallras om en överrätt frikänt den åtalade eller om en fällande dom eller beslut av någon annan anledning ändras med innebörden att den registrerade inte längre är lagförd för brottet. Detsamma gäller om kontakt- eller tillträdesförbud upphävs. I övrigt gallras uppgifterna beroende på vilken påföljd det är frågan om eller beslutets karaktär. Exempelvis gallras uppgifter om den som erhållit ett fängelsestraff tio år efter frigivningen och böter fem år efter domen. Det finns särskilda bestämmelser om gallring som gäller unga personer.

ÅM och EBM

Personuppgifter som behandlas med stöd av åklagarväsendets registerförfattning ska, enligt *21 § förordningen (2006:937) om behandling av personuppgifter inom åklagarväsendet,* gallras senast fem år efter det kalenderår då det ärende i vilken uppgiften ingår avslutades. Riksarkivet får meddela föreskrifter om undantag från bestämmelserna om gallring för att bevara material för historiska, statistiska och vetenskapliga ändamål. Sådant material ska överlämnas till en arkivmyndighet. I Riksarkivets myndighetsspecifika föreskrifter *RA-MS 2007:42* har beslutats att samtliga uppgifter i åklagarmyndigheternas ärendedatabas förda med stöd av ovan angivna förordning ska undantas från gallring.

I *11 och 12 §§ förordningen (2006:937) om behandling av personuppgifter inom åklagarväsendet* begränsas möjligheten att behandla uppgifter om brottsmisstankar. Om en förundersökning har lagts ned på grund av bristande bevisning, får uppgifter om brottsmisstanken behandlas för andra ändamål än arkivering, endast om den misstänkte enligt förundersökningsledarens bedömning fortfarande är skäligen misstänkt för brottet och uppgifterna behövs för att förundersökningen skall kunna återupptas. När ett åtal har lagts ned eller om en frikännande dom vunnit laga kraft, får uppgifter som gäller brottsmisstanken bara behandlas om förundersökningen tas upp på nytt eller det behövs för prövning av

32 Prop. 2009/10:85 s. 279

särskilt rättsmedel enligt *58 kap. rättegångsbalken* såsom exempelvis resning. Uppgifterna får naturligtvis också behandlas för arkivering.

DV

Enligt *5 § förordningen (2001:639) om registerföring m.m. vid allmän domstol med hjälp av automatiserad behandling* ska uppgifter gallras ur ett register i brottmål senast fem år efter avgörandeåret. Gallringsfunktionen i Vera är automatiserad på så sätt att gallring sker ur verksamhetsregistret när de författningsreglerade förutsättningarna är uppfyllda, dvs. i brottmål fem år efter avgörandeåret.

KV

Gallringstiderna inom KV varierar beroende på vad det är för uppgifter men de flesta gallringstider är relaterade till uppgifter som KV själv har kontroll över såsom när ett straff har verkställts. Beträffande personutredningar är dock vissa gallringstider relaterade till när målet slutligen avgjorts, *8 § förordningen (2001:682) om behandling av personuppgifter inom kriminalvården* och därför beroende av uppgifter från domstolarna.

SKV

Enligt *15 § lagen (1999:90) om behandling av personuppgifter i Skatteverkets medverkan i brottsutredningar* ska uppgifter som inte längre behövs för sitt ändamål som huvudregel gallras ur BU. Av vikt är emellertid att förundersökningar är undantagna från bestämmelsen om gallring. Dessutom får regeringen eller den myndighet som regeringen bestämmer meddela föreskrifter om att uppgifter får bevaras för historiska, statistiska eller vetenskapliga ändamål.

För förundersökningar finns istället en begränsning i hur uppgifterna får användas. Om en förundersökning lagts ned på grund av bristande bevisning får enligt *13 och 14 §§ lagen (1999:90) om behandling av personuppgifter i Skatteverkets medverkan i brottsutredningar* uppgifter om brottsmisstanken behandlas för annat ändamål än arkivering endast om den misstänkte enligt förundersökningsledarens bedömning fortfarande är skäligen misstänkt för brottet och uppgifterna behövs för att förundersökningen ska kunna tas upp på nytt. Om åtal mot en person har lagts ned eller om denne genom lagakraftvunnen dom har frikänts får uppgifter om brottsmisstanken behandlas för annat ändamål än arkivering endast om förundersökningen tas upp på nytt eller för prövning av resning eller annat särskilt rättsmedel enligt *58 kap.*

rättegångsbalken. Bestämmelserna stämmer i denna del således överens med åklagarväsendets bestämmelser.

Brå

Uppgifterna i SOR gallras inte.

Datainspektionens bedömning

Avsikten med RIF är att arbetet ska leda till effektivare ärendehantering, förbättrad kvalitet, stärkt medborgarservice och ökade möjligheter till uppföljning.[33] Datainspektionen har i sin tillsyn också funnit att arbetet i RIF har ett tydligt fokus på att skapa system för en effektivare brottmålsprocess. I arbetet prioriteras frågor som rör processen och de tekniska förutsättningarna. Frågor som rör rätten till privatliv har hittills haft en mer undanskymd roll.

Vid all elektronisk behandling av personuppgifter måste skyddet för den personliga integriteten beaktas. Inom brottmålsprocessen behandlas stora mängder av uppgifter om enskilda personer. Att uppgifterna handlar om brott innebär, enligt *dataskyddskonventionen*, att de bara får behandlas om de ges ändamålsenligt skydd. Personuppgifterna kan också vara känsliga enligt definitionen i *13 § PuL*, eller motsvarande definition i en registerförfattning, och kräva särskild restriktivitet vid behandlingen.

Merparten av de personuppgifter som nu ska överföras mellan myndigheterna elektroniskt behandlas redan hos de enskilda myndigheterna. Skillnaden när ett elektroniskt informationsflöde skapas mellan myndigheterna är att uppgifterna sprids snabbare, det är fler som kan ta del av dem i elektronisk form, det blir lättare att söka och sammanställa uppgifter, den enskilda myndighetens ansvar för uppgifterna riskerar att bli otydligare och bedömningar gällande tillåtligheten att behandla uppgifterna kan bli svårare att genomföra när uppgifterna levereras in i systemen mer eller mindre automatiskt. Det är därför viktigt att RIF-myndigheterna i sitt gemensamma arbete tar ställning till hur otillbörliga intrång i enskilda individers personliga integritet ska förhindras i det informationsflöde som skapas. Datainspektionen redogör

33 Regeringsbeslut 1996-11-21 dnr JU96/3163, 050421 Ju2004/11719/PO 021221 dnr JU2006/10392/PO

nedan för ett antal frågor som, enligt inspektionen, bör beaktas och analyseras i det fortsatta RIF-arbetet.

Vem har personuppgiftsansvar?

Inom RIF är det inte alltid den som har personuppgiftsansvaret som utvecklar systemen. Det måste ändå vara möjligt för den personuppgiftsansvarige att påverka behandlingen av personuppgifterna så att reglerna till skydd för den personliga integriteten följs.

Utgångspunkten i *3 § PuL* är att den som bestämmer om varför en behandling av personuppgifter ska ske och hur den ska ske har ansvaret för behandlingen. I de särskilda registerförfattningarna anges det ofta vem som ska ha personuppgiftsansvaret. I avsnittet om *Myndigheternas personuppgiftsansvar* har beskrivits att RPS, DV och EBM inte har personuppgiftsansvar som helt överensstämmer med grundtanken att det är den som styr över behandlingen som också har ansvaret.

Inom polis- och domstolsväsendet är det de centrala förvaltningsmyndigheterna – RPS och DV – som i stor utsträckning styr vilken typ av uppgifter som ska behandlas och hur dessa ska behandlas. Ju mer styrande systemen är desto mer bestäms av systemutvecklaren. RIF innebär att uppgiftshanteringen blir mer styrd av systemen, vilket i sin tur innebär för polisen och domstolarna att den som har det egentliga ansvaret får mindre möjlighet att påverka vilka uppgifter som ska behandlas och hur. Ansvarsfördelningen ställer stora krav på de centrala myndigheterna. Det behövs en kontinuerlig och öppen dialog med de som har getts det rättsliga personuppgiftsansvaret och de centrala myndigheterna som utvecklar systemen. Den personuppgiftsansvarige måste ha möjlighet att ta ansvaret för att systemen överensstämmer med kraven på hur personuppgifter får behandlas.

Inom åklagarväsendet använder EBM Cåbra som ärendehanteringssystem, men det är ÅM som utvecklar, förvaltar Cåbra och ÅM lagrar även EBM:s uppgifter. Vad som hör till EBM:s personuppgiftsansvar och hur det fullgörs är otydligt.

Något som bidrar till otydligheten är att det saknas personuppgiftsbiträdesavtal mellan myndigheterna trots att personuppgifter behandlas, inom såväl polis-, domstols- och åklagarväsendet, av andra myndigheter än av den som har personuppgiftsansvaret.

EBM har också en mycket otydlig beskrivning av sitt personuppgiftsansvar gentemot RPS. Det är mer ingående beskrivet i avsnittet *Myndigheterna och personuppgiftsansvaret*, men kort kan sägas att det råder osäkerhet om EBM har ansvar för alla personuppgifter i EBM:s utredningsverksamhet eller om RPS är ansvarig för de personuppgifter som behandlas i RAR och DurTvå. Någon överföring av personuppgifter till andra myndigheter sker inte från EBM:s RAR eller DurTvå och därför omfattas egentligen inte denna fråga av tillsynen. Datainspektionen anser emellertid att det är så viktigt att det klargörs vem som har personuppgiftsansvaret att problematiken ändå lyfts upp i detta sammanhang.

Är det tillåtet att elektroniskt överföra uppgifter till andra myndigheter?

Överförs sekretessbelagt material elektroniskt från en myndighet till en annan måste överföringen omfattas av sekretessbrytande bestämmelser och det måste vara tillåtet att föra över uppgifterna i elektronisk form. Myndigheterna inom RIF behöver i systemutvecklingsarbetet kontinuerligt pröva om de överföringar som ska ske har stöd i aktuella bestämmelser.

För de rättsvårdandemyndigheterna som i stor utsträckning hanterar sekretessbelagt material måste det finnas sekretessbrytande bestämmelser om uppgifterna ska överföras till andra myndigheter. Om informationen ska överföras elektroniskt måste det också vara tillåtet att lämna ut uppgifterna i den form som är aktuell. I avsnittet *Sekretessbrytande bestämmelser och elektroniskt utlämnande* beskrivs dessa regler.

Av myndigheternas enkätsvar framgår att DV och SKV analyserat de sekretessbrytandebestämmelserna utifrån sin roll i RIF och att Brå, som enbart är mottagare av uppgifter, inte behöver tillämpa bestämmelserna för egen del. Datainspektionens uppfattning är att även övriga myndigheter inom RIF7 måste analysera vad reglerna innebär för möjligheter och begränsningar för dem i RIF-arbetet. Myndigheterna behöver också gemensamt ha en samsyn vilka sekretessbrytandebestämmelser som är tillämpliga för att vara överens om vilka uppgifter som kan överföras. I analysen måste varje led ses för sig. En överföring av en uppgift från en myndighet till en annan kan inte motiveras av att uppgiften får utlämnas till en myndighet som finns senare i ledet. Det innebär till exempel att en statistikuppgift inte kan skickas från polisen via åklagare och domstol och sedan till Brå, med motiveringen att Brå behöver uppgiften.

Vad gäller formen för utlämnande så reglerar merparten av de aktuella registerförfattningarna enbart direktåtkomst. Det innebär att det oftast blir *PuL:s* regler som blir tillämpliga om det är frågan om en annan form av utlämnande, så kallat utlämnande på medium för automatiserad behandling. Enligt *PuL* är det i princip nivån på säkerheten som avgör om personuppgifter tillåts utlämnas i den formen.

Det är i sammanhanget värt att notera att skillnaderna mellan utlämnande på medium för automatiserad behandling och direktåtkomst minskar. Regeringen har uttalat i förarbeten att den tekniska utvecklingen lett till att skillnaderna mellan direktåtkomst och utlämnande på medium för automatiserad behandling blivit så liten att det ibland kan vara svårt att dra en gräns mellan dessa former av utlämnande.[34] Regeringen har också i *kommittédirektivet Integritet, effektivitet och öppenhet i en modern e-förvaltning* begärt att det ska utredas om det finns skäl att i registerförfattningarna bibehålla åtskillnaden mellan olika former av elektroniskt utlämnande.[35] I de senare registerförfattningarna har utlämnande på medium för automatiserad behandling reglerats. Såsom exempel kan nämnas bestämmelsen i *2 kap. 20 § polisdatalagen* som anger att det bara är enstaka personuppgifter som får lämnas ut på medium för automatiserad behandling om inte regeringen föreskrivit eller fattat beslut om annat.[36] I de lagförslag som bearbetas nu, gällande nya registerförfattningar för åklagarväsendet och för de allmänna domstolarna, finns det också förslag på bestämmelser som rör utlämnande på medium för automatiserad behandling.[37]

I vissa fall måste också regler ändras för att en utveckling ska vara möjlig. DV har till exempel konstaterat att registerförfattningarna måste ses över när brottmålsavgöranden ska rapporteras direkt av domstolarna istället för att det sker via RI-systemet. DV överlämnande av den anledningen en analys till SI-enheten på Justitiedepartementet den 21 september 2010. Av analysen framkommer bland annat att genom den planerade kommunikationslösningen kommer myndigheterna som tar emot domarna få mer information än idag. Det finns inte heller idag någon uppgiftsskyldighet för domstolarna som överensstämmer med den nya kommunikationslösningen. DV anger också att DV:s tänkta roll i brottmålsrapporteringen kräver författningsändring. Även Riksrevisionen påpekar i sin rapport att

34 Prop. 2007/08:160 Utökat elektroniskt informationsutbyte s. 58

35 Kommittédirektiv 2011:86 Integritet, effektivitet och öppenhet i en modern e-förvaltning

36 Motiveringen är att integritetsriskerna i vissa fall kan vara mycket likartade de som finns vid direktåtkomst prop. 2009/10:85 s.185

37 SOU 2001:100 Informationshantering och behandling av uppgifter vid domstolar – En rättslig översyn och SOU 2008:87 Åklagarväsendets brottsbekämpning, Integritet – Effektivitet

avvecklingen av RI-systemet kräver en ny reglering som ersätter *förordningen (1970:517) om rättsväsendets informationsförsörjning.*[38]

Datainspektionen anser att myndigheterna kontinuerligt måste bedöma konsekvenserna av olika former av överföringar i förhållande till reglerna som finns till skydd för den personliga integriteten i takt med att olika former av överföringar blir aktuella, såsom DV gjort beträffande avvecklingen av RI-systemet. Såväl RIF som lagstiftningsarbeten är långsiktiga projekt och det är därför viktigt att bedömningen sker i god tid. Inom RIF-arbetet kan det inte heller tas för givet att regelverken får en utformning som överensstämmer med hur systemen konstrueras. Förutom att det är frågan om grundläggande rättigheter har reglerna en EU-gemensam bas och de kan komma att få det än mer tydligt framöver om kommissionens förslag genomförs, se avsnittet *Regler till skydd för den personliga integriteten*. Byggs systemen med den förutsättningen att reglerna måste anpassas, kan det leda till att systemen måste ändras om inte de förväntade regeländringar genomförs. Sådana ändringar blir både tidsödande och kostsamma.

Hur många ska ha tillgång till uppgifterna?

Inom rättsväsendet arbetar många personer och många av dem har tillgång till något system som ingår i RIF. Systemen innehåller många personuppgifter som är integritetskänsliga. Det är därför viktigt att det prövas noga hur omfattande behörigheten ska vara. Det är också viktigt att användarens aktiviteter följs upp och att användarna informeras om vad behörigheten innebär och vilka kontrollåtgärder som vidtas.

Såsom nämnts i avsnittet *Behörighet och spårbarhet* är det totalt över 55 000 anställda inom de myndigheter som arbetar med brottmålsprocessen, varav ungefär 45 000 personer har någon form av behörighet till något av de aktuella systemen[39] . Registerförfattningarna anger ofta att behörigheten ska begränsas till vad den anställde behöver för att utföra sitt arbete. Det stämmer också överens med de grundläggande kraven på behandling av personuppgifter i *9 § PuL*. I detta fall är det framförallt *punkterna c, d och f* som är av intresse – att personuppgifter bara får samlas in för särskilt angivna ändamål, att uppgifterna inte får behandlas på något sätt som är oförenligt med de ändamål som de samlats in för

38 Riksrevisionens rapport (RiR 2011:25) It-stödet i rättskedjan s. 79
39 MR och BR är inte inkluderade

och att inte fler personuppgifter behandlas än vad som är nödvändigt med hänsyn till ändamålen.

Vilka personuppgifter en anställd har behov av är beroende av hur arbetet är organiserat. Det är idag inte ovanligt att en anställd har ett brett spektrum av uppgifter. Ett sådant exempel är de poliser som arbetar ute på fältet och som sysslar med ordningshållande, ingripanden och dessutom utreder enklare brott direkt på platsen genom mobila enheter innehållande Pust. Det finns i sådana fall ofta ett behov av att ha tillgång till en stor mängd av uppgifter. Ju mer den enskilde har tillgång till desto viktigare är det att den anställde vet i vilka situationer uppgifter får eftersökas och vad som får registreras. Det är den personuppgiftsansvarige som måste ge information till den anställde om vad behörigheten innebär. Utöver information krävs det också uppföljning av vilken behandling som sker. Vid behandling av känsliga personuppgifter ska användarens aktiviteter loggas. Av loggen ska framgå användaridentitet, tidpunkt och vilka personuppgifter användaren har haft tillgång till. Det gäller även när användaren bara läst informationen. Dessa loggar ska följas upp systematiskt och användaren ska också vara informerad om att åtgärderna loggas.[40] Såsom Dataskyddskonventionen anger hör även uppgifter om brott till de uppgifter som enligt konventionen endast får behandlas om den nationella lagstiftningen ger ett ändamålsenligt skydd, se avsnittet *Regler till skydd för den personliga integriteten* under rubriken *Dataskyddskonventionen.* Uppgifter om brott ska därför i detta sammanhang räknas in i de personuppgifter som är att betrakta som känsliga.

I exemplet om Adam så arbetar målsäganden inom rättsväsendet. Målsägandens vilja att anmäla brottet kan givetvis påverkas av hur han tror att uppgifterna kommer att behandlas i rättskedjan och vilken risk han tror att det är att uppgifterna sprids bland hans kollegor. Den som har personuppgiftsansvar måste kunna garantera målsäganden att uppgifterna bara behandlas av dem som har behov av det i sin tjänst eller av enskilda som efter sekretessprövning kan få del av uppgifterna enligt offentlighetsprincipen.

Av enkätsvaren framgår att det varierar mycket mellan myndigheterna hur styrd behörighetstilldelningen är, vilken information som ges den behörige, vad som loggas och hur loggarna följs upp. Det är bara polisen och SKV som har loggar som registrerar all behandling och som dessutom har en effektiv uppföljning av loggarna. Datainspektionen

40 Datainspektionens informationsblad Informationssäkerhet

anser att behörighetstilldelningen till de aktuella systemen måste ske nogsamt. De behöriga ska få tydlig information om vad behörigheten innebär. Systemen måste också ha loggar som visar användaridentitet, tidpunkt och vilka personuppgifter användaren har haft tillgång till. Alla system utom SOR måste också ha systematisk uppföljning. Att systematisk uppföljning inte krävs av Brå beror på att det är en mycket begränsad grupp som har tillgång till uppgifterna. En systematisk uppföljning är därför vare sig proportionerlig eller tjänar sitt syfte.

Får allmänheten del av uppgifterna?

Allmänheten har direkt tillgång till personuppgifter hos de allmänna domstolarna. Uppgifter om enskilda och sökmöjligheter utifrån uppgifter om enskilda personer måste stämma överens med reglerna till skydd för den personliga integriteten i den utsträckning som tillgången inte följer av offentlighetsprincipen.

Allmänheten har rätt att få del av handlingar som inte är sekretessbelagda enligt *2 kap 1 och 2 § tryckfrihetsförordningen och OSL*.

Allmänheten ges i vissa fall möjlighet att själv söka uppgifter i systemen. På åklagarkamrarna kan allmänheten få tillgång till Cåbra via *Allmänhetens dator* som visar ärendenummer och diarieföringsuppgifter. Polisens variant av detta är inte i bruk på grund av tekniska svårigheter. Hos de allmänna domstolarna kan allmänheten söka mål- och aktörsuppgifter i både i pågående och avslutade ärenden och mål på *Allmänhetens terminaler*. Allmänhetens tillgång till uppgifter i Vera beskrivs mer utförligt under rubriken *Allmänhetens terminal* i avsnittet *Behörighet och spårbarhet*.

Det är således bara hos domstolarna som allmänheten kan finna uppgifter om person genom allmänhetens åtkomst till systemen. Det finns därför inte någon möjlighet att kartlägga enskilda personer genom att söka i system efter system. Vad som exponeras av en myndighet kan ändå ha betydelse för den sammanlagda bilden till exempel om myndigheterna använder exempelvis gemensam identitet på brottsmisstanken. Det skulle kunna innebära en förenkling att följa och spåra specifika personer. Datainspektionen anser därför att integritetsriskerna för enskilda måste beaktas utifrån ett rättskedjeperspektiv även när det gäller allmänhetens direkta åtkomst till personuppgifter.

Domstolens uppgifter och sökmöjligheter i *Allmänhetens terminal* sträcker sig utöver vad som måste registreras enligt *5 kap. 2 § OSL* gällande inkomna eller upprättade allmänna handlingar[41] och enligt *6 kap. 6 § OSL* om serviceskyldighet vid automatiserad behandling. Offentlighetsprincipen har som syfte att enskilda ska kunna granska det allmänna. Möjligheten för allmänheten att kartlägga enskilda utifrån namn eller personnummer i system med integritetskänsliga uppgifter, väcker utifrån ett integritetsperspektiv stora betänkligheter. Det gäller inte minst möjligheten att söka på mål som är avslutade och där personen ifråga har frikänts eller där målet avskrivits för att åtalet lagts ned. Att offentlighetsprincipen har företräde framför *PuL* innebär inte att det är möjligt att inskränka rätten till privatliv utöver vad som är direkt föreskrivet beträffande rätten att ta del av allmänna handlingar.[42] Personuppgiftsansvaret för *Allmänhetens terminal* har den domstol där terminalen finns. I tillsynen avseende RIF är det DV som varit föremål för tillsyn. Datainspektionen gör därför i detta sammanhang endast detta påpekande.

Hur länge får uppgifterna behandlas?

För myndigheterna finns ofta begränsningar i hur länge de får behandla uppgifter i sin verksamhet även om det är frågan om uppgifter som ska bevaras genom arkivering. I vissa fall påverkar andra myndigheters beslut hur länge uppgifterna får behandlas. Det är viktigt att myndigheterna inom RIF får de uppgifter som behövs så att uppgifterna inte behandlas längre tid än tillåtet.

Många uppgifter som behandlas inom rättsväsendet ska inte gallras i den meningen att de ska tas bort för gott. Tvärtom ska merparten av uppgifterna bevaras genom arkivering. Det hindrar inte att det finns begränsningar för hur uppgifterna i övrigt får behandlas.

För alla myndigheter i RIF7 utom Brå finns det begränsningar för hur länge uppgifterna får behandlas i verksamheten, vilket beskrivs i avsnittet *Bevarande av uppgifter.* När begränsningen inträffar påverkas

41 Enligt 5 kap. 2 § OSL ska allmänna handlingar registreras så att det framgår datum då handlingen kom in eller upprättades, diarienummer eller annan beteckning handlingen fått vid registreringen, i förekommande fall uppgifter om handlingens avsändare eller mottagare och i korthet vad handlingen rör. Uppgifter om handlingens avsändare eller mottagare, och i korthet vad handlingen rör ska utelämnas eller särskiljas om det behövs för att registret i övriga delar ska kunna hållas tillgängligt för allmänheten.

42 Se Förvaltningsrätten i Stockholm dom 2012-04-24 mål nr 33893-10 Länsstyrelsen i Västra Götalands län mot Datainspektionen avseende Tillsyn enligt PuL, dels en fråga om medarbetarnas tillgång till samtliga handlingar i handläggningsplattformen som är allmänna och offentliga och dels allmänhetens tillgång till Diarium Utsidan på Internet.

av beslut, domar eller verkställighet. För att behandlingen inte ska pågå längre än tillåtet behövs information från den som fattar beslutet, avkunnar domen eller genomför verkställigheten. RIF har hittills arbetat framåt i kedjan vilket innebär att den återkoppling som behövs för att rensa uppgifter inte alltid tillgodoses. En sådan problematik noterades vid beredningen av *polisdatalagen*. Det fick till följd att övergångsbestämmelser infördes i *polisdatalagen* som angav att vissa regler som begränsar polisens möjlighet att i sin brottsbekämpande verksamhet behandla personuppgifter inte behöver tillämpas förrän den 1 januari 2015.[43] Anledningen till att övergångsbestämmelserna ansågs nödvändiga var att polisen inte kunde få den återkoppling från åklagarmyndigheten eller domstolarna som krävs för att uppfylla reglerna. I avsnittet *Bevarande av uppgifter* under rubriken RPS beskrivs detta utförligare. Det finns också ett långt citat från förarbetena till *polisdatalagen* i vilken det direkt hänvisas till att det arbete som Rådet för rättsväsendets informationsförsörjning bedriver, ska åstadkomma en rutin för elektronisk återkoppling till polisen av beslut av myndigheter i senare led i rättskedjan.

I den första etappen har det trots uttalandet i förarbetena till *polisdatalagen* inte bedrivits något arbete inom RIF för att åstadkomma de återkopplingar som behövs för att kunna begränsa tillgången till personuppgifter i enlighet med bestämmelserna. Regeringen har i sitt beslut att ge myndigheterna i uppdrag att utföra den andra etappen av RIF, angett att myndigheterna ska skapa funktioner i arbetet som säkerställer integritetsskyddet.[44] Datainspektionen förutsätter att det innebär att de erforderliga återkopplingarna kommer prioriteras i den andra etappen av RIF.

Är uppgifterna riktiga och behandlas de korrekt?

Om flera system använder samma personuppgifter är det viktigt att det finns ett tydligt ansvar för att uppgifterna är riktiga. Det är också viktigt att personuppgifterna behandlas på ett korrekt sätt.

Ett syfte med RIF är att de uppgifter som hanteras ska bli mer korrekta än idag, eftersom inte var och en av myndigheterna behöver mata in dem. Risken för slarvfel ska på så sätt minska. Det är bra och Datainspektionens uppfattning är att det elektroniska informationsflödet kan bidra till att behandlingen av personuppgifter blir mer rätt. Samtidigt finns det en risk att den personuppgiftsansvarige inte tar

43 Övergångsbestämmelserna till polisdatalagen 5 punkterna b och c
44 Regeringsbeslut 2012-10-11 Uppdrag att utveckla rättsväsendets informationsförsörjning Ju2012/6639/SI

samma ansvar för uppgifter som överförs från system till system mellan myndigheter som för uppgifter som registreras av den egna myndigheten. I avsnittet *Riktiga uppgifter och korrekt behandling* beskrivs två JK-ärenden. I det ena använde en tingsrätt uppgifter som inkommit från åklagaren utan att göra en egen bedömning och kom därför att behandla uppgifterna om en person felaktigt. I det andra ärendet kontrollerade inte polisen att de uppgifter som de skickade vidare i rättskedjan var aktuella.

PuL har som grundläggande krav på behandling av personuppgifter, att uppgifterna alltid ska behandlas på ett korrekt sätt och vara riktiga.[45] Det är den som har personuppgiftsansvar som har ansvar för behandlingen och det går därför inte att vid felaktigheter hänvisa vare sig till systemet i sig eller till den myndighet som översänt uppgifterna. Det är viktigt att uppgifter om personer som överförs mellan myndigheterna inte ”*hamnar*” fel utan får en korrekt behandling. Det är också viktigt att myndigheterna kommer överens om hur rättelser och uppdateringar ska ske så att det får genomslag i hela rättskedjan.

I exemplet med Adam i avsnittet *Brottmålsprocessen – ett exempel* illustreras hur snabbt och till hur många system uppgifterna sprids. Är de antecknade uppgifterna oriktiga så är det viktigt att uppgifterna lika snabbt rättas på alla ställen där de förekommer. Det är också vikigt att Adam inte slussas mellan myndigheterna om han begär rättelse.

Hur behandlas känsliga personuppgifter?

Myndigheterna måste skapa system eller rutiner som innebär att känsliga personuppgifter bara behandlas när det är tillåtet enligt de regler som gäller för respektive myndighet.

Känsliga personuppgifter får enligt *PuL:s* huvudregel inte behandlas elektroniskt. Myndigheterna inom RIF tillåts i sina respektive registerförfattningar att behandla känsliga personuppgifter under vissa förutsättningar. Flera registerförfattningar anger att uppgifter om en person kan kompletteras med känsliga personuppgifter om det är absolut nödvändigt för syftet med behandlingen, se avsnittet *Känsliga personuppgifter*.

I enkätsvaren anger merparten av myndigheterna att de inte behandlar känsliga personuppgifter i strukturerad form. Vid behandling av ostrukturerat material är det många regler i *PuL* som inte behöver beaktas,

45 9 § första stycket punkterna b och g PuL

däribland reglerna om känsliga personuppgifter. I RIF används dock begreppet strukturerat på ett annat sätt än i *PuL*. I *PuL* är det själva samlingen av uppgifter som avgör om den är att anse som strukturerad eller inte och inte den enskilda personuppgiften eller handlingen som ingår i samlingen, vilket beskrivs i avsnittet *Regler till skydd för den personliga integriteten* under rubriken *Personuppgiftslagen*. Allt material som ingår eller ska ingå i systemen i brottmålsprocessen är därför strukturerat enligt *PuL*.

Att det inte är ovanligt att det i brottmålsprocessen behandlas känsliga personuppgifter enligt definitionen i *13 § PuL* kan illustreras av exemplet om Adam. I målet gällande Adam kan det i misshandelsdelen finnas såväl rättsläkarutlåtande avseende målsägandens skador som uppgifter om en homosexuell relation i förhören. De uppgifterna ska behandlas med den restriktivitet som reglerna kräver gällande känsliga personuppgifter.

För att kunna iaktta restriktivitet måste det finnas kännedom om att det förekommer känsliga personuppgifter i de överförda uppgifterna. Inom RIF finns det inte någon markering eller överenskommelse som gör det möjligt att särskilt beakta känsliga personuppgifter. För att myndigheterna ska kunna uppfylla de särskilda krav som finns för att få behandla känsliga personuppgifter behövs det såväl en analys inom RIF om vad som är känsliga personuppgifter och när dessa kan komma att behandlas. Myndigheterna behöver också komma överens om på vilket sätt de särskilda krav som finns för känsliga personuppgifter ska beaktas vad gäller uppgifter som överförs mellan myndigheterna.

Kan RIF stärka skyddet för den personliga integriteten?

De moderna IT-systemen styr användarna i stor utsträckning. Det är därför viktigt att kraven på integritetsskydd beaktas och så långt det är möjligt byggs in i systemen.

I och med att IT-systemen får större kapacitet ökar både integritetsriskerna, men också möjligheterna att skapa integritetsskydd genom att införa skyddande funktioner i systemen. Det har kommissionen tagit fasta på och enligt förslaget till dataskyddsdirektiv för de brottsbekämpande myndigheterna ska *Data protection by design* användas vid systemutveckling. [46] Även regeringen har i uppdraget avseende den andra etappen av RIF uppgett att myndigheterna ska skapa funktioner

46 Kommissionens förslag till dataskyddsdirektiv för de brottsbekämpande myndigheterna (KOM (2012) 10 slutlig) artikel 19

i arbetet som säkerställer integritetsskyddet.[47] Datainspektionen har i en vägledning från januari 2012 *Inbyggd integritet – Privacy by design* beskrivit hur IT-system kan bygga in mekanismer för att skydda den personliga integriteten.

Om skyddet för privatlivet integreras i systemen kan RIF ha en positiv effekt på personuppgiftsbehandlingen. Det kan handla om att systemen vägleder användaren så att det blir lätt att göra rätt, men det kan också vara frågan om att integritetsskyddande funktioner byggs in i systemen. Exempel på funktioner som måste vara en del av systemen är loggning, sökfunktioner och vissa behörighetsbegränsningar. Beaktas inte behoven av integritetsskydd när systemen utvecklas kan det leda till onödiga kostnader och tidsödande arbetsinsatser för att inarbeta skydden i efterhand. Det är därför viktigt att konsekvenserna för den enskildes personliga integritet kartläggs fortlöpande i arbetet med RIF och att lösningar utarbetas som stärker skyddet för den personliga integriteten.

Sammanfattning

Datainspektionens bedömning är att frågor som rör behandling av personuppgifter och respekten för den enskildes integritet hittills har haft en alltför undanskymd roll i RIF-arbetet. Det är därför positivt att regeringen inför den andra etappen uttryckligen angett att myndigheterna ska skapa funktioner i arbetet som säkerställer integritetsskyddet.

Moderna IT-system kan skapas så att de ger effektivitet inte bara åt processen utan också åt integritetsskyddet. RIF är därför en möjlighet att integrera skyddet för personuppgifter med systemen om så kallad *Inbyggd integritet – Privacy by design* används. RIF kan till exempel innebära att de personuppgifter som behandlas blir mer korrekta och att de hanteras mer enhetligt och rättssäkert. Samtidigt finns det flera risker för den personliga integriteten när stora system som många personer har behörighet till kopplas samman. Uppgifterna sprids snabbt och till många, ansvaret kan bli otydligt och när uppföljningen av ärenden och mål förenklas och förbättras kan även enskilda individer enklare kartläggas. Om rätten till privatliv ska respekteras måste det i arbetet med RIF kontinuerligt ske analyser av vad olika överföringar innebär

47 Regeringsbeslut 2012-10-11 Uppdrag att utveckla rättsväsendets informationsförsörjning Ju2012/6639/SI

för personuppgiftsbehandlingen och hur reglerna till skydd för den personliga integriteten efterlevs. Utifrån dessa analyser behöver myndigheterna sedan skapa integritetsskydd, i första hand genom funktioner i systemen och i andra hand genom överenskommelser mellan myndigheterna och införande av rutiner.

Datainspektionen anser att myndigheterna i RIF särskilt bör vidta följande åtgärder:

- analysera det rättsliga stödet för att överföra sekretessbelagda personuppgifter i elektronisk form, avseende både befintliga överföringar och planerade
- tilldela behörigheter, informera användarna, logga och följa upp loggarna i enlighet med vad som är reglerat avseende behandling av personuppgifter för respektive myndighet
- skapa funktioner i systemen eller överenskommelser och rutiner för att rätta personuppgifter som överförts till andra myndigheter
- skapa funktioner i systemen eller överenskommelser och rutiner för att säkerställa att överförda personuppgifter behandlas på ett korrekt sätt
- analysera behovet av återkoppling och skapa dessa så att de begränsningar som ska gälla för verksamheternas personuppgiftsbehandling kan efterlevas
- analysera vilka känsliga personuppgifter som överförs och skapa funktioner i systemen eller överenskommelser och rutiner som säkerställer att uppgifterna bara behandlas när det är tillåtet enligt de regler som gäller för respektive myndighet.

Kontakta Datainspektionen

E-post: datainspektionen@datainspektionen.se Webb: www.datainspektionen.se
Tfn 08-657 61 00. Postadress: Datainspektionen, Box 8114, 104 20 Stockholm.

Datainspektionen