

Till statsrådet och chefen för Justitiedepartementet

Chefen för Justitiedepartementet, statsrådet Ask, har den 20 juni 2007 beslutat uppdra åt överåklagaren Gunnel Lindberg att biträda departementet med att utarbeta en promemoria som behandlar frågan om godkännande av rambeslut om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete.

Härmed överlämnas promemorian Antagande av rambeslut om skydd av personuppgifter som behandlas inom ramen för polis-samarbete och straffrättsligt samarbete.

Uppdraget är därmed slutfört.

Stockholm i april 2008

Gunnel Lindberg

Innehåll

Till statsrådet och chefen för Justitiedepartementet	3
1 Sammanfattning	13
2 Bakgrund	15
3 Allmänt om innehållet i utkastet till rambeslut	17
3.1 Allmänt om utkastet till rambeslut	17
3.2 Rambeslutets innehåll	19
3.2.1 Syfte och tillämpningsområde	19
3.2.2 Grundläggande regler för behandlingen	20
3.2.3 Behandling av känsliga personuppgifter	21
3.2.4 Automatiserade beslut	21
3.2.5 Närmare om behandlingen av personuppgifter	22
3.2.6 Överföring av uppgifter till tredje land	23
3.2.7 Överföring av uppgifter till privata subjekt	24
3.2.8 Information till den registrerade	25
3.2.9 Tillgång till rättsmedel, skadestånd och sanktioner	26
3.2.10 Sekretess och tystnadsplikt	27
3.2.11 Säkerheten vid behandlingen	27
3.2.12 Tillsyn	28
3.2.13 Förhållandet mellan rambeslutet och andra instrument	29

3.2.14	Övriga frågor.....	30
4	Gällande rätt.....	31
4.1	Behandling av personuppgifter i allmänhet	31
4.1.1	Allmänt om regleringen.....	31
4.1.2	Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna	31
4.1.3	Europiska unionens stadga om de grundläggande rättigheterna.....	32
4.1.4	Dataskyddskonventionen.....	33
4.1.5	Riktlinjer från OECD	34
4.1.6	Dataskyddsdirektivet.....	34
4.2	Personuppgiftslagen.....	36
4.2.1	Lagens tillämpningsområde.....	36
4.2.2	Grundläggande krav för behandlingen	37
4.2.3	Tillåten och otillåten behandling	38
4.2.4	Behandling av personuppgifter i ostrukturerat material	39
4.2.5	Behandling av känsliga uppgifter	39
4.2.6	Uppgifter om brott och behandling av personnummer	40
4.2.7	Information till den registrerade.....	40
4.2.8	Rättelse	41
4.2.9	Säkerhet vid behandlingen.....	41
4.2.10	Överföring av personuppgifter till tredje land.....	42
4.2.11	Tillsyn	42
4.2.12	Sanktioner	43
4.3	En lagstiftning i förändring	44
4.4	Behandling av personuppgifter inom polisen.....	44
4.4.1	Europarådets rekommendation om användningen av personuppgifter inom polissektorn	44

4.4.2	Allmänt om polisens behandling av personuppgifter	45
4.4.3	Polisdatalagen	46
4.4.4	Lagen om belastningsregister.....	50
4.4.5	Lagen om misstankeregister.....	51
4.4.6	Lagen om Schengens informationssystem	53
4.4.7	Lagen om passagerarregister	55
4.4.8	Förordningen om ordningsbotsregister	55
4.4.9	Förordningen om strafförelägganderegister	56
4.4.10	Andra register som förs i polisens brottsbekämpande verksamhet	57
4.4.11	Register med annat primärt ändamål.....	59
4.5	Andra myndigheters behandling av personuppgifter för brottsbekämpning.....	60
4.5.1	Tullverket	60
4.5.2	Kustbevakningen	64
4.5.3	Skatteverket.....	65
4.5.4	Åklagarväsendet.....	68
4.6	Lagstiftning om behandling av personuppgifter inom andra verksamhetsområden som berörs av rambeslutet	70
4.6.1	Allmänna utgångspunkter	70
4.6.2	Kriminalvården	71
4.6.3	Domstolsväsendet	74
4.7	Tillsyn över personuppgiftsbehandling	77
4.7.1	Datainspektionen.....	77
4.7.2	Säkerhets- och integritetsskyddsnämnden	78
4.8	Sekretess och tystnadsplikt	79
4.8.1	Allmänt om sekretesslagens reglering	79
4.8.2	Sekretess i brottsbekämpande verksamhet	79
4.8.3	Sekretess för vissa register	81
4.8.4	Sekretess vid handläggning i domstol.....	84

4.8.5	Sekretess för verkställighet av straffrättsliga påföljder.....	84
4.8.6	Sekretess för personuppgifter	85
4.8.7	Utlämnande av sekretessbelagda uppgifter	85
4.8.8	Bestämmelser om tystnadsplikt i registerförfattningar	88
4.9	Regler om informationssäkerhet.....	88
5	Internationellt samarbete	91
5.1	Allmänna utgångspunkter	91
5.2	Regler om användningsbegränsningar	91
5.3	Samarbete i den brottsbekämpande verksamheten	93
5.3.1	Lagstiftningen om polissamarbete	93
5.3.2	Lagen om internationellt tullsamarbete.....	97
5.4	Lagstiftningen om internationellt rättsligt samarbete	99
5.4.1	Internationell rättslig hjälp i brottmål.....	99
5.4.2	Överlämnande från Sverige enligt en europeisk arresteringsorder	100
5.4.3	Erkännande och verkställighet av frysningsbeslut.....	102
5.4.4	Rambeslut om en europeisk bevisinhämtningsorder.....	102
5.4.5	Rambeslut om utbyte av information ur kriminalregister	103
5.5	Lagstiftning om samarbete i fråga om verkställighet av påföljder	105
5.5.1	Allmänt.....	105
5.5.2	Internationella verkställighetslagen	105
5.5.3	Rambeslut om överförande av frihetsberövande påföljder inom Europeiska unionen	107
5.5.4	Nordiska verkställighetslagen	107

5.5.5	Övertagande av straffverkställighet till följd av en arresteringsorder	108
5.5.6	Straffverkställighet i Sverige av straff utdömda av internationella tribunaler och domstolar	109
5.5.7	Samarbete rörande kriminalvård i frihet.....	109
5.6	Samarbetet med vissa internationella organ	111
5.6.1	Interpol.....	111
5.6.2	Europol.....	112
5.6.3	Eurojust.....	114
5.6.4	European Judicial Network	115
5.6.5	World Customs Organization.....	115
6	Förslag till ny lagstiftning om behandling av personuppgifter hos de brottsbekämpande myndigheterna m.m.	117
6.1	Förslag till ny lag om behandling av personuppgifter i polisens brottsbekämpande verksamhet.....	117
6.1.1	Tillämpningsområdet.....	117
6.1.2	Grundläggande bestämmelser.....	118
6.1.3	Gemensamt tillgängliga uppgifter	119
6.1.4	Sökbegränsningar.....	121
6.1.5	Behandling av känsliga personuppgifter.....	122
6.1.6	Informationsutbyte och sekretess	122
6.1.7	Gallring.....	123
6.1.8	Särskilda register	124
6.1.9	Särskilda bestämmelser för Säkerhetspolisen.....	125
6.1.10	Tillsyn.....	127
6.1.11	Förslag till lag om polisens spaningsregister.....	128
6.1.12	Ikraftträdande	129
6.2	Förslag till ny lagstiftning om Schengens informationssystem.....	130
6.3	Genomförande av Prümrådsbeslutet	131

6.4	VIS.....	132
6.5	Rambeslut om förenklat informations- och underrättelseutbyte	134
6.6	Förslag till ny reglering av behandlingen av personuppgifter inom Kustbevakningen.....	135
	6.6.1 Allmänt om förslaget.....	135
	6.6.2 Den fortsatta handläggningen.....	136
6.7	Förslag till ny lagstiftning om behandling av personuppgifter inom domstolsväsendet.....	138
6.8	Utredning om ny lagstiftning om behandling av personuppgifter inom åklagarväsendet	139
6.9	Integritetsskyddskommitténs synpunkter och förslag....	139
7	Pågående förhandlingsarbete inom Europeiska unionen.....	141
7.1	Europol	141
7.2	Eurojust	142
7.3	European Judicial Network.....	142
7.4	Passagerarregister.....	143
8	Genomförande av rambeslutet	145
8.1	Inget genomgripande behov av ny lagstiftning.....	145
8.2	Personuppgiftslagen och dess roll.....	148
	8.2.1 Allmänt om personuppgiftslagen.....	148
	8.2.2 Räcker personuppgiftslagens regler?	149
8.3	Rambeslutets syfte och tillämpningsområde.....	151
8.4	Ändamålen med behandlingen	156

8.5	Behandling av känsliga personuppgifter	166
8.6	Korrigerings av personuppgifter.....	168
8.7	Överföring av uppgifter till tredje land eller till internationella organisationer	173
8.8	Överföring av uppgifter till privata parter.....	177
8.9	Gallring.....	179
8.10	Användningsbegränsningar	184
8.11	Information till den registrerade.....	189
8.12	Tillgång till rättsmedel.....	194
8.13	Säkerheten vid behandlingen.....	197
8.14	Sekretess	199
8.15	Tillsyn	201
8.16	Skadestånd	205
8.17	Sanktioner.....	207
8.18	Automatiserade beslut	211
8.19	Övriga frågor.....	213
9	Antagande av rambeslutet.....	215
9.1	Godkännande av rambeslutet.....	215
9.2	Skälen för att några lagförslag inte läggs fram.....	217
10	Ekonomiska konsekvenser	221

Bilaga 1	Utkastet till rambeslut om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete ...	223
Bilaga 2	Utkast till rådsbeslut	259

1 Sammanfattning

I promemorian föreslås att riksdagen ska godkänna ett inom Europeiska unionen upprättat utkast till rambeslut om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete.

Utkastet till rambeslut innehåller bestämmelser som syftar till att förstärka skyddet för behandling av personuppgifter inom nu nämnda områden, i det vidare syftet att kunna förbättra det gränsöverskridande utbytet av information om brottsbekämpning mellan medlemsstaterna. Rambeslutet utgör ett viktigt komplement till andra instrument om polisiärt och straffrättsligt samarbete.

Utkastet innehåller bestämmelser om allmänna principer för behandlingen av personuppgifter, behandling av känsliga personuppgifter, rättelse, radering och gallring av personuppgifter, information till den registrerade samt skadestånd och sanktioner. I stora delar motsvarar utkastet till rambeslutet innehållet i det s.k. dataskyddsdirektivet, som har genomförts i svensk rätt genom personuppgiftslagen.

I promemorian övervägs, på ett mera allmänt plan, vilka lagändringar som kan bli nödvändiga med anledning av rambeslutet. Promemorian innehåller inga lagförslag.

2 Bakgrund

Den 4 november 2004 antog Europeiska rådet det s.k. Haagprogrammet för stärkt frihet, säkerhet och rättvisa i Europeiska unionen. Rådet uttalade där att en förstärkning av frihet, säkerhet och rättvisa kräver en innovativ strategi i fråga om gränsöverskridande utbyte av information om brottsbekämpning. En princip bör vara att en tjänsteman vid en brottsbekämpande myndighet i en medlemsstat ska göra befintlig information tillgänglig för motsvarande befattningshavare i en annan stat om han eller hon behöver informationen för att utföra sina uppgifter.

Ett effektivare polissamarbete och rättsligt samarbete måste emellertid balanseras av grundläggande rättigheter, särskilt rätten till ett privatliv och rätten till skydd av personuppgifter. I Haagprogrammet uppmanades kommissionen att lägga fram förslag till genomförandet av principen om tillgänglighet för att förbättra det gränsöverskridande utbytet av information om brottsbekämpning mellan medlemsstaterna, under strikt iakttagande av centrala villkor i fråga om skydd av personuppgifter. Detta återspeglas i rådets och kommissionens handlingsplan för genomförande av Haagprogrammet.

Den 4 oktober 2005 presenterade kommissionen ett förslag till rambeslut om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete. Efter ingående förhandlingar, där medlemsstaterna inte kunde enas, omarbetades förslaget på ett genomgripande sätt under det tyska ordförandeskapet. De fortsatta förhandlingarna fördes med det omarbetade förslaget som utgångspunkt.

De materiella bestämmelserna i utkastet till rambeslut är till stora delar identiska med motsvarande artiklar i Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter (dataskyddsdirektivet).

Förutom medlemsstaterna inom Europeiska unionen har även Island, Norge och Schweiz deltagit i förhandlingarna om utkastet till rambeslut, som ett led i det utvidgade Schengensamarbetet.

Europaparlamentet har yttrat sig över det ursprungliga förslaget den 27 september 2006 och över det reviderade förslaget den 6 juni 2007. Europeiska datatillsynsmannen har avgett tre yttranden över utkastet till rambeslut, den 19 december 2005, den 29 november 2006 och den 27 april 2007.

I slutet av år 2007 nåddes en politisk principöverenskommelse om innehållet i utkastet till rambeslut, med reservation för vissa ändringar bl.a. i preambeln. Sverige lämnade i samband med det en parlamentarisk granskningsreservation. Utkastet till rambeslut sändes sedan till Europaparlamentet för förnyat yttrande. Efter Europaparlamentets yttrande över det slutliga utkastet till rambeslut ska en granskning av texten göras av Europeiska unionens språkexperter, de s.k. juristlingvisterna.

Regeringen har under förhandlingsarbetet fortlöpande informerat och samrått med riksdagen. Företrädare för Justitiedepartementet har sammanträtt med Justitieutskottet och justitieministern har vid sammanträde i EU-nämnden redogjort för förhandlingsarbetet och den svenska positionen.

Utkastet till rambeslut i den senaste svenska översättningen bifogas som *bilaga 1* till denna promemoria.

3 Allmänt om innehållet i utkastet till rambeslut

3.1 Allmänt om utkastet till rambeslut

Utkastet till rambeslut om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete (i fortsättningen rambeslutet) utgör ett viktigt komplement till olika instrument om utvidgat polisiärt samarbete och rättsligt samarbete inom Europeiska unionen med inriktning på utökat gränsöverskridande informationsutbyte.

Inledningsvis framhålls att gemensamma insatser inom polis-samarbetet och rörande straffrättsligt samarbete gör det nödvändigt att behandla information samtidigt som det måste finnas regler om skydd för personuppgifter. Gemensamma normer för behandling och skydd av personuppgifter kan både bidra till ett effektivare samarbete och värna grundläggande rättigheter som rätten till privatliv och rätten till skydd för personuppgifter. Det framhålls vidare att utbytet av personuppgifter inom ramen för polissamarbete och rättsligt samarbete bör bygga på tydliga regler som stärker förtroendet mellan myndigheterna och garanterar att informationen skyddas, samtidigt som enskildas grundläggande rättigheter respekteras. Vidare konstateras att befintliga instrument på europeisk nivå inte är tillräckliga och att data-skyddsdirektivet inte är tillämpligt på behandling av personuppgifter inom det nu aktuella området.

I skäl 6 a anges att det är medlemsstaternas avsikt att – trots att rambeslutets ska tillämpas på uppgifter som har överförts till

eller gjorts tillgängliga mellan medlemsstaterna – se till att den nivå på dataskydd som gäller för nationell behandling motsvarar vad som föreskrivs i rambeslutet. Rambeslutet hindrar dock inte medlemsstaterna från att ha starkare skydd för behandling av personuppgifter än vad som anges i rambeslutet. Vidare bör tillnärmningen inte leda till ett svagare skydd för personuppgifter än det som medlemsstaternas nuvarande lagstiftning ger utan tvärtom syfta till att garantera en hög skyddsnivå inom hela unionen (skäl 7).

Av skäl 15 a framgår att rambeslutet medger att offentlighetsprincipen beaktas vid genomförandet.

Preambeln är omfattande och innehåller bl.a. många hänvisningar till andra fördrag och rättsakter. Detta hör samman med att dessa inte sällan innehåller bestämmelser om dataskydd av delvis samma slag som rambeslutet. Grundtanken med rambeslutet är att detta ska tillämpas i stället för de dataskyddsbestämmelser som finns i många andra instrument.

Vissa undantag från denna huvudregel har dock ansetts nödvändiga. Undantag görs framför allt för sådana rättsakter som innehåller en komplett och enhetlig uppsättning dataskyddsbestämmelser där dataskyddet regleras mera detaljerat än i rambeslutet. Det pekas särskilt på de rättsakter som reglerar Europol, Eurojust, Schengen Information System (SIS) och Tullinformationssystemet (TIS). Likaså undantas dataskyddsbestämmelser som reglerar automatisk överföring av DNA-profiler samt uppgifter ur fingeravtrycksregister och fordonsregister (skäl 24 a och b).

Det framhålls särskilt att rambeslutet inte påverkar Europarådets konvention av den 28 januari 1981 om skydd för enskilda vid automatisk databehandling av personuppgifter eller tilläggsprotokollet till denna konvention och inte heller Europarådets konventioner om straffrättsligt samarbete (skäl 19).

3.2 Rambeslutets innehåll

3.2.1 Syfte och tillämpningsområde

I *artikel 1* anges rambeslutets syfte och tillämpningsområde. Syftet är att säkerställa en hög skyddsnivå för fysiska personers fri- och rättigheter när det gäller behandling av personuppgifter inom ramen för polissamarbete och straffrättsligt samarbete.

Tillämpningsområdet för rambeslutet är personuppgifter som översänds eller görs tillgängliga, eller har översänts eller gjorts tillgängliga,

- mellan medlemsstater,
- av medlemsstater för organ eller informationssystem som har upprättats inom Europeiska unionen, eller
- för behöriga myndigheter i medlemsstater av sådana organ eller informationssystem.

Endast behandling av personuppgifter som utförs helt eller delvis automatiskt samt annan behandling av personuppgifter som ingår i eller kommer att ingå i register faller under tillämpningsområdet. Från tillämpningsområdet undantas också viktiga nationella säkerhetsintressen och särskild underrättelseverksamhet inom området nationell säkerhet.

Rambeslutet är inte heller tillämpligt på sådana uppgifter som en medlemsstat har fått från en annan stat men som har sitt ursprung i den mottagande staten (skäl 6 b).

Rambeslutet hindrar, som nyss nämnts, inte att en medlemsstat har strängare regler för personuppgifter som behandlas eller samlas in på nationell nivå.

Artikel 2 innehåller definitioner av vissa grundläggande begrepp som används i rambeslutet. De begrepp som definieras är

- personuppgifter,
- behandling av personuppgifter,
- blockering,
- register med personuppgifter,
- registerförare,
- mottagare,

- den registrerades samtycke,
- behöriga myndigheter,
- registeransvarig,
- markering, och
- avidentifiering.

Definitionerna motsvarar i allt väsentligt de definitioner som finns i dataskyddsdirektivet.

3.2.2 Grundläggande regler för behandlingen

I *artikel 3* läggs vissa grundläggande principer för personuppgiftsbehandlingen fast, bl.a. huvudregeln att uppgifter inte får behandlas för annat ändamål än det ursprungliga.

I punkten 1 föreskrivs att personuppgifter får samlas in bara för särskilda, uttryckligt angivna och berättigade ändamål och endast behandlas för det ändamål som låg till grund för insamlingen av dem. Behandlingen måste dessutom vara befogad, adekvat och relevant för ändamålet. Behandling för ett annat ändamål än det ursprungliga tillåts dock enligt punkten 2 om

- vidarebehandlingen inte är oförenlig med det ändamål för vilket uppgifterna samlades in,
- vederbörande myndighet har författningsenlig rätt att behandla sådana uppgifter, och
- behandlingen är nödvändig och står i proportion till ändamålet.

Dessutom får uppgifter behandlas för historiska, statistiska eller vetenskapliga ändamål, under förutsättning att lämpliga säkerhetsåtgärder föreskrivs, såsom att uppgifterna avidentifieras.

Enligt *artikel 4* ska personuppgifter rättas om de är felaktiga samt, om det är möjligt och nödvändigt, kompletteras eller uppdateras. Uppgifterna ska enligt huvudregeln raderas eller avidentifieras när de inte längre behövs för de ändamål för vilka de insamlats eller vidarebehandlats. Arkivering i en separat datamiljö enligt nationell lagstiftning faller dock utanför. Detta förutsätter dock enligt skäl 8 b att uppgifterna inte längre kan användas för

att förebygga, uppdaga, utreda eller lagföra brott eller för verkställighet av straffrättsliga påföljder.

Uppgifterna ska inte raderas utan blockeras, om det finns skäl att anta att radering skulle kunna påverka den registrerades lagliga intressen. Blockerade uppgifter får bara behandlas för det ändamål som hindrade att de raderades. Om uppgifterna ingår i ett domstolsbeslut eller i underlaget för ett sådant beslut ska rättelse, radering eller blockering utföras enligt nationella bestämmelser.

I *artikel 6* föreskrivs att medlemsstaterna ska fastställa lämpliga tidsfrister för radering av personuppgifter eller för omprövning av fortsatt lagring. Det ska finnas bestämmelser som tillgodoser att gallringsfristerna iakttas.

3.2.3 Behandling av känsliga personuppgifter

Artikel 7 reglerar behandling av s.k. känsliga uppgifter, dvs. uppgifter om ras eller etniskt ursprung, politisk uppfattning, religiös eller filosofisk övertygelse eller medlemskap i fackförening samt uppgifter som rör hälsa och sexualliv. Sådana uppgifter får behandlas endast om det är absolut nödvändigt och den nationella lagstiftningen erbjuder tillräckliga rättssäkerhetsgarantier.

3.2.4 Automatiserade beslut

I *artikel 8* behandlas automatiserade beslut. Beslut, som har rättsliga följder för en person eller som annars har märkbara verkningar för personen och som grundas enbart på automatiserad behandling, som är avsedda att bedöma egenskaper hos personen är endast tillåtna om den registrerades intresse skyddas genom lagstiftning.

3.2.5 Närmare om behandlingen av personuppgifter

Artikel 9 innehåller bestämmelser om kvaliteten på personuppgifter som översänds eller görs tillgängliga. Myndigheterna ska vidta alla rimliga åtgärder för att tillse att personuppgifter som är felaktiga, ofullständiga eller inte längre aktuella inte överförs eller görs tillgängliga. Så långt möjligt ska myndigheterna kontrollera personuppgifternas kvalitet innan de översänds eller görs tillgängliga.

I största möjliga utsträckning ska ytterligare information lämnas som möjliggör för mottagaren att bedöma uppgifternas korrekthet, fullständighet, aktualitet och tillförlitlighet. I de fall där uppgifter lämnas utan föregående begäran ska mottagaren bekräfta om uppgifterna är nödvändiga. Om det visar sig att felaktiga uppgifter har tillhandahållits, eller om överföringen av dem har varit lagstridig, ska mottagaren underrättas så snabbt som möjligt. Personuppgifterna ska genast rättas, raderas eller blockeras enligt bestämmelserna i artikel 4.

Enligt *artikel 10* ska den myndighet som sänder över eller gör personuppgifter tillgängliga ange de gallringsfrister som gäller enligt nationell lagstiftning. Mottagaren är skyldig att radera eller blockera uppgifterna när fristen har löpt ut, eller att kontrollera om uppgifterna fortfarande behövs. Kravet på radering eller blockering gäller inte om uppgifterna behövs för pågående brottsutredning, lagföring eller straffverkställighet. Om den sändande myndigheten inte har angett någon gallringsfrist ska nationell lagstiftning tillämpas.

Utöver de nu angivna kraven ska behandlingen också uppfylla kraven i artikel 3 punkten 2, vilket innebär att behandlingen inte får vara oförenlig med det ursprungliga ändamålet, att behandlingen ska utföras av en behörig myndighet samt att behandlingen ska vara nödvändig och proportionerlig.

I *artikel 12* regleras vidarebehandling av uppgifter som erhållits från en annan medlemsstat. Sådana uppgifter får behandlas endast för följande andra ändamål än de för vilka de översändes eller gjordes tillgängliga, nämligen

- för att förebygga, uppdaga, utreda eller lagföra andra brott eller verkställa andra straffrättsliga påföljder,
- för andra rättsliga eller administrativa förfaranden som är direkt relaterade till förebyggande, uppdagande, utredning eller lagföring av brott eller verkställighet av straffrättsliga påföljder,
- för att förhindra ett omedelbart och allvarligt hot mot allmän säkerhet, eller
- med förhandsmedgivande från den sändande staten, eller från den registrerade, varje annat ändamål.

Behandling för historiska, statistiska eller vetenskapliga ändamål är tillåten under förutsättning att medlemsstaten föreskriver tillräckligt skydd som t.ex. avidentifiering av personuppgifterna.

När det är tillåtet med vidarebehandling inkluderar det behandling hos en tillsynsmyndighet (skäl 11 b).

Om det enligt den sändande statens lagstiftning gäller särskilda restriktioner för visst informationsutbyte enligt nationell rätt, ska enligt *artikel 13*, mottagaren underrättas om dessa restriktioner. Mottagaren ska respektera restriktionerna. Andra restriktioner än de som gäller för motsvarande nationellt informationsutbyte får inte tillämpas.

Enligt *artikel 15* ska mottagaren, på begäran, informera den myndighet som översänt eller gjort personuppgifterna tillgängliga om behandlingen av dem.

3.2.6 Överföring av uppgifter till tredje land

I *artikel 14* regleras överföring av uppgifter till tredje land eller till internationella organ. Medlemsstaterna ska tillse att personuppgifter som har överförts från eller gjorts tillgängliga av en annan medlemsstat får överföras till tredje land eller till internationella organ endast om

- detta är nödvändigt för att förebygga, uppdaga, utreda eller lagföra brott eller verkställa straffrättsliga påföljder,

- den mottagande myndigheten i tredje land eller det internationella organet ansvarar för sådan verksamhet,
- den medlemsstat från vilken personuppgifterna erhållits har gett samtycke till överföringen, och
- det aktuella tredje landet eller internationella organet har en adekvat skyddsnivå för behandlingen av personuppgifterna.

Varje medlemsstat får bestämma formerna för samtycke, exempelvis om generellt samtycke ska ges för viss typ av uppgifter eller viss vidarebehandling (skäl 11 a).

Utan föregående samtycke får överföring äga rum endast om uppgifterna är avgörande för att avvärja ett omedelbart och allvarligt hot mot allmän säkerhet i en medlemsstat eller ett tredje land eller för särskilt viktiga intressen för en medlemsstat och samtycke inte hinner inhämtas. Den myndighet som ska ge samtycke ska genast informeras.

Dessutom får överföring ske, trots att skyddsnivån hos mottagaren inte anses vara adekvat, bl.a. om det tredje landet eller det internationella organet erbjuder en skyddsnivå för personuppgiftsbehandling som har bedömts vara tillräcklig med hänsyn till medlemsstatens nationella lagstiftning.

Skyddsnivån ska bedömas med hänsyn till samtliga omständigheter. Särskild hänsyn ska tas till bl.a. uppgifternas art, ändamålet med behandlingen och den tid denna förväntas ta, ursprungslandet och slutdestinationen.

3.2.7 Överföring av uppgifter till privata subjekt

I *artikel 14 a* regleras på motsvarande sätt överföring av personuppgifter till privata subjekt i medlemsstaterna. Sådan överföring av uppgifter som erhållits från eller gjorts tillgängliga av en annan medlemsstat får äga rum endast om

- myndigheten i den sändande staten har gett sitt samtycke,
- den registrerades legitima intressen inte hindrar överföring, och

- i det enskilda fallet en överföring till det privata subjektet är nödvändig för att myndigheten ska kunna
 - * fullgöra sina lagenliga uppgifter,
 - * förebygga, uppdaga, utreda eller lagföra brott eller verkställa straffrättsliga påföljder,
 - * avvärja ett omedelbart och allvarligt hot mot allmän säkerhet, eller
 - * hindra allvarlig skada på enskildas rättigheter.

Den myndighet som överför personuppgifter till ett privat subjekt ska underrätta detta om de enda ändamål för vilka uppgifterna får behandlas.

3.2.8 Information till den registrerade

Medlemsstaterna ska enligt *artikel 16* tillse att den registrerade, i enlighet med nationell lagstiftning, informeras om insamlingen och behandlingen av personuppgifter. Har personuppgifter översänts eller gjorts tillgängliga mellan medlemsstater, får varje medlemsstat i enlighet med sin lagstiftning begära att den andra medlemsstaten inte informerar den registrerade utan föregående samtycke av den sändande staten.

Varje person har, på begäran som görs med rimliga intervall, enligt *artikel 17* rätt att kostnadsfritt och utan hinder och större dröjsmål åtminstone få

- a) bekräftelse från den personuppgiftsansvarige eller från den nationella tillsynsmyndigheten om huruvida personuppgifter om den registrerade har överförts eller gjorts tillgängliga och uppgift om mottagaren eller kategorin av mottagare av personuppgifterna samt att få del av de uppgifter som behandlas, eller
- b) bekräftelse från den nationella tillsynsmyndigheten att alla nödvändiga kontroller har genomförts.

Medlemsstaterna får införa bestämmelser som begränsar tillgången till information enligt a) om begränsningarna, med hänsyn tagen till den berörda personens intressen, innebär en nöd-

vändig och proportionerlig åtgärd för att inte hindra bl.a. brottsutredning, lagföring och straffverkställighet samt för att skydda allmän säkerhet, nationell säkerhet eller den registrerades eller annans fri- och rättigheter.

Om information inte kan lämnas ska den registrerade informeras skriftligen om detta och om skälen för vägran. Underrättelse kan underlåtas i vissa fall. Den registrerade ska underrättas om sin rätt att överklaga beslutet.

3.2.9 Tillgång till rättsmedel, skadestånd och sanktioner

I *artikel 18* regleras enskildas rätt till rättelse, radering eller blockering av uppgifter enligt artiklarna 4, 9 och 10. Medlemsstaterna ska ange om den registrerade har rätt att vända sig direkt till den personuppgiftsansvarige i sådana frågor eller måste gå via den nationella tillsynsmyndigheten. Ett beslut av den personuppgiftsansvarige att inte vidta rättelse, radering eller blockering ska vara skriftligt och innehålla uppgift om vilka möjligheter den registrerade har att anföra klagomål eller begära prövning av beslutet. Den registrerade ska informeras om huruvida den personuppgiftsansvarige har agerat korrekt eller inte. Medlemsstaterna får även föreskriva att den registrerade enbart ska informeras av den nationella tillsynsmyndigheten om att en kontroll har gjorts. Om en registrerad bestrider riktigheten i en uppgift och dess riktighet inte kan bekräftas får uppgiften i stället markeras.

I *artikel 19* föreskrivs att en person som har lidit skada av en otillåten personuppgiftsbehandling, eller en behandling som inte är förenlig med nationell lagstiftning, har rätt till ersättning för skadan från den personuppgiftsansvarige eller annan myndighet enligt nationell lagstiftning. Om en behörig myndighet i en medlemsstat har överfört personuppgifter, får mottagaren i förhållande till den skadelidande inte hävda att de överförda uppgifterna var felaktiga för att undgå ansvar. Om mottagaren utger ersättning för skada som orsakats på grund av felaktigt översända personuppgifter, ska den översändande myndigheten ersätta

mottagaren för utgivet skadestånd, varvid ska beaktas att felet kan ha begåtts av mottagaren.

Utan hinder av administrativa förfaranden, ska en registrerad enligt *artikel 20* ha tillgång till rättsmedel för brott mot de rättigheter som garanteras i nationell lagstiftning.

Enligt *artikel 24* ska medlemsstaterna vidta åtgärder för att säkerställa genomförandet av rambeslutet genom att föreskriva effektiva, proportionella och avskräckande sanktioner mot den som bryter mot bestämmelserna. Det står medlemsstaterna fritt att välja vilken typ av sanktion som ska gälla för överträdelser (skäl 15).

3.2.10 Sekretess och tystnadsplikt

Artikel 21 reglerar sekretess vid behandlingen. Personer som ges tillgång till personuppgifter som omfattas av rambeslutets tillämpningsområde får behandla uppgifterna endast i egenskap av anställda vid eller på instruktion från en behörig myndighet, utom i fall där behandlingen är författningsreglerad. En person som arbetar för en behörig myndighet skall följa alla dataskyddsregler som gäller för myndigheten i fråga.

Personalen hos tillsynsmyndigheten ska enligt *artikel 25* punkten 4 vara underkastade tystnadsplikt som ska gälla även efter att de slutat sin anställning där.

3.2.11 Säkerheten vid behandlingen

Säkerheten vid behandling regleras i *artikel 22*. Medlemsstaterna ska tillse att behöriga myndigheter genomför tillräckliga tekniska och organisatoriska åtgärder för att skydda personuppgifter mot både oavsiktlig och avsiktlig förstöring, ändring samt otillåtet röjande, särskilt när behandlingen innefattar överföring genom nätverk eller tillgängliggörande genom direktåtkomst, och mot

all annan otillåten behandling. Särskild hänsyn ska tas till de risker som behandlingen medför och arten av uppgifter.

Medlemsstaterna ska i fråga om automatisk databehandling vidta lämpliga åtgärder för att skapa

- åtkomstskydd för utrustningen,
- databärarkontroll,
- lagringskontroll,
- användarkontroll,
- åtkomstkontroll,
- kommunikationskontroll,
- indatakontroll,
- överföringskontroll,
- återställande, samt
- driftssäkerhet och dataintegritet.

Medlemsstaterna ska sörja för att endast sådana personer utses att behandla personuppgifter som kan garanteras vidta nödvändiga tekniska eller organisatoriska åtgärder av detta slag. Personuppgifter får behandlas av annan endast på grundval av lagstiftning eller skriftligt avtal.

Varje överföring av personuppgifter ska enligt *artikel 11* loggas eller dokumenteras på annat sätt. Loggar och annan dokumentation ska på begäran tillhandahållas den nationella tillsynsmyndigheten.

3.2.12 Tillsyn

Varje medlemsstat ska enligt *artikel 25* utse en eller flera nationella tillsynsmyndigheter som ska ansvara för rådgivning och kontroll av tillämpningen. Det finns inget som hindrar att den myndighet som är tillsynsmyndighet enligt dataskyddsdirektivet utses till tillsynsmyndighet också enligt rambeslutet (skäl 16 a).

Tillsynsmyndigheterna ska agera självständigt i sin tillsynsroll. En tillsynsmyndighet ska ha vissa i artikeln angivna verktyg. Myndigheten ska ha möjlighet att utreda, möjlighet att uttala sig om tillämpningen och att ingripa exempelvis genom att kräva

radering eller att förbjuda behandling samt möjlighet att agera rättsligt vid överträdelser.

Tillsynsmyndigheterna ska behandla klagomål från enskilda rörande ingrepp i fri- och rättigheter avseende personuppgiftsbehandling. Den klagande ska informeras om utgången av ärendet.

Medlemsstaterna ska vidare enligt *artikel 23* tillse att den nationella tillsynsmyndigheten får tillfälle att yttra sig innan en helt ny typ av behandling av personuppgifter påbörjas i de fall där behandlingen rör känsliga personuppgifter, eller om behandlingen innebär exceptionella risker för grundläggande fri- och rättigheter, särskilt registrerades rätt till privatliv för den registrerade, framför allt om behandlingen sker med hjälp av ny teknologi, nya tillämpningsmekanismer eller processer.

3.2.13 Förhållandet mellan rambeslutet och andra instrument

Artikel 27 behandlar förhållandet mellan rambeslutet och andra överenskommelser med tredje land. Rambeslutet påverkar inte sådana bilaterala eller multilaterala avtal som Europeiska unionen eller någon medlemsstat har ingått före antagandet av rambeslutet. Vid tillämpningen av sådana avtal ska dock kravet i artikel 14 punkterna 1 c och 2 på förhandsmedgivande respekteras när personuppgifter översänds till tredje land.

Artikel 27 b reglerar förhållandet mellan rambeslutet och befintliga rättsakter. I fråga om sådana rättsakter som har antagits med stöd av artikel 6 i EU-fördraget innan rambeslutet trätt i kraft, och som reglerar överföring av personuppgifter mellan medlemsstaterna eller behöriga myndigheters tillgång till informationssystem och där särskilda villkor gäller för mottagande medlemsstaters användning av sådana uppgifter, ska villkoren gälla framför reglerna i rambeslutet om uppgifterna härrör från en annan medlemsstat. Det sagda gäller dock endast sådana villkor som är mer restriktiva än de som föreskrivs i rambeslutet (skäl 24 b).

Vidare framhålls i skäl 47 att rambeslutet inte påverkar dataskyddet enligt dataskyddsdirektivet (se avsnitten 4.14 och 4.2.1) och annan bindande EG-rättslig lagstiftning.

3.2.14 Övriga frågor

Medlemsstaterna ska enligt *artikel 28* genomföra rambeslutet inom två år efter antagandet. Rambeslutet träder i kraft den tjugonde dagen efter publiceringen i Europeiska unionens officiella tidning.

I *artikel 27 a* föreskrivs att när rambeslutet har varit i kraft under tre år ska en utvärdering ske. Kommissionen, som särskilt ska kontrollera genomförandet av tillämpningsområdet i artikel 1 punkten 2, ska redovisa utvärderingen till rådet och Europaparlamentet.

4 Gällande rätt

4.1 Behandling av personuppgifter i allmänhet

4.1.1 Allmänt om regleringen

Enligt 2 kap. 3 § regeringsformen får anteckning om medborgare i allmänt register inte utan hans samtycke grundas enbart på hans politiska åskådning. Vidare ska varje medborgare, i den utsträckning som närmare anges i lag, skyddas mot att hans personliga integritet kränks genom att uppgifter om honom registreras med hjälp av automatiska databehandling.

Personuppgiftslagen (1998:204) innehåller generella riktlinjer för behandling av personuppgifter, oavsett ändamålet med behandlingen. Lagen ersatte den tidigare datalagen (1973:289), då dataskyddsdirektivet (se avsnitt 4.1.6) genomfördes i svensk rätt.

Övergångsreglerna till personuppgiftslagen var generösa. För manuell behandling av personuppgifter som omfattas av lagen och som hade påbörjats före ikraftträdandet började lagen gälla först i oktober 2007 och på polisområdet gäller datalagen alltjämt för vissa register.

4.1.2 Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna

Den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) gäller sedan år 1995 som svensk lag. Två av artiklarna i kon-

ventionen, artikel 8 och artikel 13, har betydelse för myndigheters rätt att behandla personuppgifter.

Artikel 8 föreskriver att var och en har rätt till respekt bl.a. för sitt privat- och familjeliv. En offentlig myndighet får inte inskränka åtnjutandet av denna rättighet annat än med stöd av lag och om det i ett demokratiskt samhälle är nödvändigt med hänsyn till statens säkerhet, den allmänna säkerheten, landets ekonomiska välbefinnande eller till förebyggande av oordning eller brott eller till skydd för hälsa eller moral eller för andra personers fri- och rättigheter.

Kravet på att inskränkningen ska ha lagstöd anses innebära att inskränkningen måste vara utformad med sådan precision att den är i rimlig utsträckning förutsebar. En rättighetsinskränkande tolkning av lagen ska kunna förutses och lagen ska vara allmänt tillgänglig. De syften för vilka intrång tillåts har tolkats ganska extensivt av Europadomstolen, men domstolen avgör vad som kan anses vara nödvändigt för att tillgodose ett i och för sig legitimt syfte. Ett rättighetsintrång bedöms således vara nödvändigt endast om det svarar mot ett mycket angeläget socialt behov och om det står i rimlig proportion till det syfte som ska uppnås.

I artikel 13 föreskrivs att var och en, vars i konventionen angivna fri- och rättigheter kränkts, ska ha tillgång till ett effektivt rättsmedel inför en nationell myndighet. Detta gäller även om kränkningen förövats av någon som utövat offentlig myndighet. Innebörden av artikeln är att den enskilde ska ha tillgång till en nationell instans för att få saken prövad och kunna erhålla rättelse. Prövningen kan utföras av domstol, men något krav på domstolsprövning uppställs inte. Prövning av en stats regering eller av en förvaltningsmyndighet kan alltså vara tillräcklig.

4.1.3 Europiska unionens stadga om de grundläggande rättigheterna

I Europeiska unionens stadga från år 2000 bekräftas de rättigheter som har sin grund i medlemsstaternas gemensamma författ-

ningstraditioner och internationella förpliktelser samt i Fördraget om Europeiska unionen och gemenskapsfördragen, såsom Europakonventionen och Europarådets sociala stadgor och rättspraxis vid Europeiska domstolen för de mänskliga rättigheterna. Syftet med stadgan är att kodifiera de grundläggande fri- och rättigheter som Europeiska unionen erkänner. Stadgan är enbart en politisk viljeförklaring och således inte rättsligt bindande.

Däremot är stadgan bindande för Europeiska unionens egna organ och institutioner samt för medlemsstaterna när de tillämpar unionsrätten.

I stadgans artikel 8 föreskrivs att var och en har rätt till skydd av de personuppgifter som rör honom eller henne. Dessa uppgifter ska behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim eller lagenlig grund. Var och en har rätt att få tillgång till insamlade uppgifter som rör honom eller henne och att få rättelse av dem. En oberoende myndighet ska kontrollera att reglerna efterlevs.

4.1.4 Dataskyddskonventionen

Europarådets konvention från år 1981 om skydd för enskilda vid automatisk databehandling av personuppgifter (dataskyddskonventionen) brukar ses som en precisering av artikel 8 i Europakonventionen. Konventionen trädde ikraft den 1 oktober 1985. Samtliga medlemsstater i Europeiska unionen har ratificerat konventionen.

Dataskyddskonventionens syfte är att säkerställa den enskildes rätt till personlig integritet och förbättra förutsättningarna för ett fritt informationsflöde över gränserna. Den innehåller principer för dataskydd som parterna måste uppfylla i sin nationella lagstiftning. Personuppgifter som är föremål för automatisk databehandling ska hämtas in och behandlas på ett korrekt sätt för särskilt angivna ändamål. Uppgifterna måste vara relevanta

och förenliga med ändamålen. Vidare ska uppgifterna vara riktiga och aktuella och uppgifterna får inte heller bevaras längre än vad som är nödvändigt för ändamålen. Känsliga personuppgifter får behandlas endast om nationell lagstiftning ger ett tillfredsställande skydd. Det gäller t.ex. uppgifter om enskildas ras, politiska tillhörighet eller religiösa tro samt uppgifter om brott.

Konventionen föreskriver att lämpliga skyddsåtgärder ska vidtas för att hindra avsiktlig eller otillåten förstörelse m.m. Vidare finns bestämmelser om registrerades möjligheter till insyn i register och möjligheter att få uppgifter rättade.

År 2001 antog Europarådets ministerkommitté ett tilläggsprotokoll till dataskyddskonventionen. Detta innehåller bestämmelser om dataskyddsmyndigheter och överföring av personuppgifter mellan länder. Sverige har ratificerat tilläggsprotokollet. Inom Europarådet har det vidare utarbetas en rad rekommendationer om skydd för personuppgifter inom olika områden, bl.a. såvitt avser polisens verksamhet (se avsnitt 4.4.1).

4.1.5 Riktlinjer från OECD

Organisationen för ekonomiskt samarbete och utveckling (OECD) har också utarbetat internationella riktlinjer för integritetsskydd och flöde av persondata. Ett antal internationella organisationer och företag har antagit egna regler om dataskydd som bygger på OECD:s riktlinjer. Riktlinjerna motsvarar i princip de bestämmelser som finns i dataskyddskonventionen.

4.1.6 Dataskyddsdirektivet

Syftet med 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) är att skapa en gemensam, hög nivå på integritetsskyddet för att därigenom möjliggöra

ett fritt flöde av personuppgifter medlemsländerna emellan. Inom de ramar som anges i direktivet får medlemsländerna närmare precisera villkoren för när behandling av personuppgifter får förekomma.

Direktivet innehåller en rad materiella bestämmelser som reglerar all hantering av personuppgifter. I direktivet finns bl.a. generella regler om vilka krav som ställs vid behandling av personuppgifter, när sådan behandling är tillåten, information till den registrerade, rättelse av personuppgifter, säkerheten vid behandlingen och överföring av personuppgifter till tredje land, dvs. till en stat utanför Europeiska unionen och EES.

Direktivet är inte tillämpligt på sådan behandling av personuppgifter som faller utanför gemenskapsrätten. Det innebär att bl.a. verksamhet som rör allmän säkerhet, statens säkerhet eller verksamhet inom straffrättens område faller utanför direktivets tillämpningsområde.

Dataskyddsdirektivet genomfördes i svensk rätt genom införandet av personuppgiftslagen, som presenteras närmare i avsnitt 4.2.

Den svenska personuppgiftslagen är generellt tillämplig och omfattar även sådan behandling som faller utanför gemenskapsrätten. Samtidigt som personuppgiftslagen infördes tillskapades särskilda lagar och andra författningar som reglerar behandlingen av personuppgifter för ett visst verksamhetsområde, för en viss typ av register eller för ett enda register. Polisdatalagen och lagarna om belastningsregister och misstankeregister är exempel på detta. Skälet till att dessa lagar infördes var att lagstiftaren valde att ge personuppgiftslagen generell tillämpning samtidigt som det fanns behov av att ha avvikande regler för vissa verksamheter eller register.

Lagen tillämpas därför även på behandling av personuppgifter i polisens och andra brottsbekämpande myndigheters verksamhet. I polisdatalagen och motsvarande författningar för Skatteverkets och Kustbevakningens brottsbekämpande verksamhet finns dock en särreglering som till stora delar ersätter personuppgiftslagen. Motsvarande gäller för personuppgiftsbehand-

lingen inom åklagarväsendet, domstolsväsendet och kriminalvården. Vissa grundläggande regler som exempelvis definitioner gäller dock även för dessa verksamheter. För Tullverkets del har valts en annan lagstiftningsmodell men resultatet är detsamma, nämligen att personuppgiftslagen delvis gäller.

4.2 Personuppgiftslagen

4.2.1 Lagens tillämpningsområde

Genom datalagen introducerades begreppet personregister som ett centralt begrepp i svensk datalagstiftning. Med personregister avsågs i den lagen register, förteckning eller andra anteckningar som förs med hjälp av automatisk databehandling och som innehåller personuppgift som kan hänföras till den som avses med uppgiften. Genom datalagen blev uttrycket "register" den allmänt använda termen för datoriserade uppgiftssamlingar. Uttrycket finns i många författningar som reglerar myndigheters användning av automatisk databehandling i verksamheten, t.ex. i polisdatalagen.

Det traditionella registerbegreppet har med tiden kommit att kritiseras alltmer. En orsak till detta är att begreppet även har en teknisk anknytning och därför kan ha olika innebörd för olika yrkesgrupper. Vidare för uttrycket register tankarna till på visst sätt organiserade eller systematiserade samlingar av uppgifter. Numera är det inte lika relevant att betrakta samlingar av uppgifter i elektronisk form på detta sätt. Uppgifter kan t.ex. införas helt ostrukturerat och oorganiserat i olika filer i en dator utan att detta förhindrar en effektiv hantering av uppgifterna för olika sammanställningar. Sökning i sådana filer görs normalt genom fritextsökning.

I personuppgiftslagen används inte begreppet register utan det talas i stället om behandling av personuppgifter. Lagen reglerar hur personuppgifter får hanteras. Den ska tillämpas på all helt eller delvis automatiserad behandling av personuppgifter. Dess-

utom är den tillämplig på manuell behandling av personuppgifter som ingår, eller är avsedda att ingå, i en strukturerad samling av personuppgifter vilka är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

Personuppgiftslagen har, som nyss nämnts, ett vidare tillämpningsområde än dataskyddsdirektivet, eftersom den reglerar även sådan verksamhet som faller utanför gemenskapsrätten. Enligt 2 § gäller särreglering i lag eller förordning framför bestämmelserna i personuppgiftslagen. Sådan särreglering finns framför allt i olika registerförfattningar. Utgångspunkten har varit att myndighetsregister med ett stort antal registrerade och ett särskilt känsligt innehåll ska regleras särskilt i lag (prop. 1990/91:60 s. 50 och KU 1990/91:11 s. 11).

Behandling av uppgifter om juridiska personer (som definitionsmässigt inte utgör personuppgifter) eller behandling som en fysisk person utför i verksamhet av rent privat natur omfattas inte av personuppgiftslagen (3 § resp. 6 §). Även viss annan behandling faller utanför tillämpningsområdet (7 och 8 §§).

4.2.2 Grundläggande krav för behandlingen

I 9 § slås fast vissa grundläggande krav för all behandling av personuppgifter. Sådana uppgifter ska alltid behandlas på ett korrekt och lagligt sätt samt i enlighet med god sed. Personuppgifter ska samlas i och behandlas för särskilda, uttryckligt angivna ändamål. Efter insamlingen får uppgifterna inte behandlas för något annat ändamål som är oförenligt med det ändamål för vilket uppgifterna samlades in (den s.k. finalitetsprincipen). De personuppgifter som behandlas ska vidare vara riktiga och relevanta i förhållande till ändamålen med behandlingen och får inte heller vara fler än vad som är nödvändigt med hänsyn till ändamålen med behandlingen. Om det är nödvändigt ska uppgifterna vara aktuella. Om personuppgifterna inte uppfyller dessa krav, ska den personuppgiftsansvarige vidta alla rimliga åtgärder för att utplåna, blockera eller rätta uppgifterna.

Personuppgifter får inte sparas längre än nödvändigt med hänsyn till de ändamål för vilka de behandlas. Därefter ska de aidentifieras eller förstöras. Eftersom personuppgiftslagen är subsidiär till annan lagstiftning får uppgifter inte aidentifieras eller förstöras på annat sätt om det strider mot annan lagstiftning, t.ex. tryckfrihetsförordningens bestämmelser om allmänna handlingar.

4.2.3 Tillåten och otillåten behandling

I lagen finns en uttömmande uppräkningslista av de fall där behandling av personuppgifter är tillåten (10–12 §§). Personuppgifter får alltid behandlas om den registrerade har gett sitt samtycke. Återkallar personen sitt samtycke får ytterligare personuppgifter om denne inte registreras.

I vissa fall får personuppgifter behandlas även om den registrerade inte har gett sitt samtycke. En förutsättning i dessa fall är att behandlingen är nödvändig för ändamålen.

Personuppgifter får behandlas i samband med ett avtal med den registrerade, när det behövs för att fullgöra avtalet eller när det behövs för att på den registrerades begäran vidta åtgärder innan avtalet träffas. Vidare får behandling utföras om det är nödvändigt för att den personuppgiftsansvarige ska kunna fullgöra en rättslig skyldighet. Dessutom får personuppgifter behandlas för att skydda vitala intressen för den registrerade. Likaså får personuppgifter behandlas om det är nödvändigt för att den personuppgiftsansvarige, eller en tredje man till vilken personuppgifter lämnas ut, ska kunna utföra en arbetsuppgift i samband med myndighetsutövning.

Slutligen får personuppgifter behandlas om en avvägning ger vid handen att den personuppgiftsansvariges berättigade intresse av behandling väger tyngre än den registrerades intresse av skydd.

4.2.4 Behandling av personuppgifter i ostrukturerat material

Personuppgiftslagen innehåller en särskild regel om behandling av personuppgifter i ostrukturerat material som gör undantag från ett flertal av lagens bestämmelser (5 a §). För sådan behandling gäller inte en hanterings- utan en missbruksmodell. Sådan behandling av personuppgifter i ostrukturerat material som innebär en kränkning av den registrerades personliga integritet får inte utföras.

4.2.5 Behandling av känsliga uppgifter

Enligt 13 § personuppgiftslagen förbjuds behandling av känsliga personuppgifter. Med detta avses uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening samt uppgifter som rör hälsa eller sexualliv.

Förbudet mot behandling av känsliga uppgifter är inte undantagslöst. I 14–19 §§ anges under vilka förutsättningar sådana uppgifter får behandlas.

Om den registrerade har gett sitt uttryckliga samtycke till behandlingen eller på ett tydligt sätt offentliggjort de känsliga uppgifterna får de behandlas (15 §). Vidare görs undantag för nödvändig behandling, bl.a. för att den personuppgiftsansvarige ska kunna fullgöra skyldigheter eller utöva rättigheter inom arbetsrätten, om den registrerades eller annans vitala intressen ska kunna skyddas och den registrerade inte kan lämna samtycke till behandlingen eller om rättsliga anspråk ska kunna fastställas, göras gällande eller försvaras (16 §).

Undantag görs också för ideella organisationer med politiskt, filosofiskt, religiöst eller fackligt syfte, som får behandla uppgifter om sina medlemmar (17 §).

Likaså finns det undantag för behandlingen av känsliga personuppgifter för hälso- och sjukvårdsändamål (18 §) samt forsk-

ning och statistik (19 §). Regeringen, eller den myndighet regeringen bestämmer, får också föreskriva ytterligare undantag från förbudet i 13 §, om det behövs med hänsyn till ett viktigt allmänt intresse (20 §).

4.2.6 Uppgifter om brott och behandling av personnummer

Det är enligt 21 § personuppgiftslagen förbjudet för andra än myndigheter att behandla sådana personuppgifter om lagöverträdelse som innefattar brott, domar i brottmål, straffprocessuella tvångsmedel eller administrativa frihetsberövanden. Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om undantag från förbudet. Likaså kan i enskilda fall undantag medges.

Uppgifter om personnummer och samordningsnummer får enligt 22 § behandlas utan samtycke bara när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl.

4.2.7 Information till den registrerade

Personuppgiftslagen innehåller ett flertal bestämmelser som syftar till att genom information trygga den enskildes rätt att kontrollera om behandling av personuppgifter om honom eller henne pågår. Den personuppgiftsansvariges skyldighet att själv lämna information till de registrerade gäller i första hand uppgifter som den registrerade själv har lämnat (23 §). Har uppgifterna samlats in från annan källa, skall den registrerade informeras när uppgifterna noteras, eller om avsikten med behandlingen är att lämna ut dem till tredje man, när uppgifterna lämnas ut första gången (24 §). Information behöver dock inte lämnas om det finns bestämmelser om registrerandet eller utlämnande av uppgifterna i lag eller författning. Information behöver heller

inte lämnas om det skulle vara omöjligt eller kräva en opropor-tionerligt stor arbetsinsats.

Informationen ska omfatta uppgift om vem som är person-uppgiftsansvarig, ändamålet med behandlingen samt all övrig information som den registrerade behöver för att kunna ta till-vara sina rättigheter i samband med behandlingen (25 §). Infor-mationsskyldigheten omfattar bara sådana uppgifter som den registrerade inte redan känner till.

Den personuppgiftsansvarige är vidare skyldig att efter ansö-kan, en gång per år, gratis informera om uppgifter om sökanden behandlas eller inte, ändamålet med behandlingen, vilka uppgif-ter som behandlas, varifrån dessa kommer och till vem de lämnas ut (26 §). Någon information behöver dock inte lämnas om per-sonuppgifter som endast behandlas i löpande text som ännu inte fått sin slutliga utformning eller utgör minnesanteckning, utom i de fall där uppgifterna har lämnats ut till tredje man eller – i fråga om behandling i löpande text – har behandlats mer än ett år.

Informationsskyldigheten gäller inte heller i de fall där upp-gifterna omfattas av sekretess eller tystnadsplikt (27 §).

4.2.8 Rättelse

Personuppgifter som är felaktiga eller ofullständiga eller som annars inte har behandlats i enlighet med personuppgiftslagen, ska på begäran av den registrerade rättas, utplånas eller blockeras av den personuppgiftsansvarige (28 §). Om felaktiga personupp-gifter har lämnats ut till tredje man, ska denne i vissa fall infor-meras om korrigeringen.

4.2.9 Säkerhet vid behandlingen

I 30 och 31 §§ personuppgiftslagen finns allmänna bestämmelser om säkerheten vid behandling av personuppgifter. Bestämmel-serna avser att trygga både den tekniska säkerheten och att de

personer som behandlar uppgifterna har tillräckliga instruktioner för att behandla uppgifterna på ett korrekt sätt. Den personuppgiftsansvarige har stort ansvar för säkerheten.

4.2.10 Överföring av personuppgifter till tredje land

Enligt 33 § personuppgiftslagen är det förbjudet att till tredje land föra över personuppgifter under behandling om landet inte har en adekvat nivå för skyddet av personuppgifterna. Förbudet gäller också överföring av personuppgifter för behandling i tredje land. Frågan om skyddsnivån är adekvat ska bedömas med hänsyn till samtliga omständigheter som har samband med överföringen. I paragrafen anges vilka omständigheter som ska tillmätas särskild vikt.

I 34 § anges vissa undantag från förbudet i 33 §. Ett viktigt undantag är att det är tillåtet att föra över personuppgifter för användning enbart i en stat som har anslutit sig till dataskyddskonventionen (se avsnitt 4.1.4 om konventionen). I 35 § finns vissa bemyndiganden som avser möjligheten att besluta om ytterligare undantag i förbudet i 33 §. I bilagor till personuppgiftsförordningen anges vissa länder som enligt särskilt beslut av Europeiska gemenskapernas kommission anses ha en adekvat skyddsnivå för behandlingen av personuppgifter. Till dessa hör bl.a. länder som Schweiz och överföringar till vissa mottagare i USA och Kanada.

4.2.11 Tillsyn

Datainspektionen är tillsynsmyndighet enligt såväl artikel 28 i dataskyddsdirektivet som personuppgiftslagen. Datainspektionen är som regel också tillsynsmyndighet för sådan behandling av personuppgifter som är reglerad i särskilda registerförfattningar. Inspektionen har till uppgift att bl.a. verka för att människor skyddas mot att den personliga integriteten kränks genom

behandling av personuppgifter. Datainspektionen informerar bl.a. om gällande regler och utövar tillsyn över att reglerna efterlevs samt att ger råd och hjälp åt personuppgiftsombud. I 43–47 §§ personuppgiftslagen finns närmare bestämmelser om tillsynsmyndighetens befogenheter, t.ex. om rätten att meddela vite och om möjligheten att ytterst förbjuda viss behandling.

4.2.12 Sanktioner

Om behandling av personuppgifter i strid med personuppgiftslagen orsakar skada för den registrerade har vederbörande rätt till skadestånd från den personuppgiftsansvarige (48 §). Rätten till ersättning omfattar både personskada, sakskada och ren förmögenhetsskada som kränkningen av den personliga integriteten kan ha medfört. Skadeståndsansvaret är i princip strikt. Den registrerade behöver bara visa att det förekommit en felaktig behandling och att denna skadat eller kränkt honom eller henne.

Lagen innehåller också en straffbestämmelse. Till böter eller fängelse i högst sex månader döms bl.a. den som

- behandlar personuppgifter i strid med bestämmelserna om behandling av känsliga personuppgifter eller
- för över personuppgifter till tredje land i strid med bestämmelserna i 33–35 §§.

Straffansvaret för behandling av personuppgifter i ostrukturerat material är begränsat och omfattar bara otillåten behandling av känsliga personuppgifter och uppgifter om lagöverträdelse samt överföring av personuppgifter till tredje land som inte har en adekvat nivå för skyddet av personuppgifter.

I ringa fall döms inte till ansvar. Vidare får ansvar inte utkrävas för en gärning som omfattas av ett vitesföreläggande enligt lagen.

4.3 En lagstiftning i förändring

Detta kapitel innehåller en redovisning av den nu gällande lagstiftningen om behandling av personuppgifter i den brottsbekämpande verksamheten och vissa angränsande verksamhetsområden där rambeslutets reglering har betydelse. Det bör redan här framhållas att inom flera av dessa områden är lagstiftningen föremål för översyn eller under omarbetning. Av det skälet är redovisningen här av de särskilda författningarna om behandling av personuppgifter inte så ingående som den annars skulle ha varit. För en närmare beskrivning av gällande rätt och av den nuvarande behandlingen av personuppgifter hänvisas till de betänkanden som rör respektive verksamhetsområde. Polisens brottsbekämpande verksamhet redovisas i Ds 2007:43. En beskrivning av Kustbevakningens personuppgiftsbehandling finns i SOU 2006:18. För domstolarna finns motsvarande redogörelse i SOU 2001:100. Åklagarväsendets personuppgiftsbehandling redovisas i direktiven till översyn (dir. 2007:126).

I avsnitt 6 redovisas regeringens förslag om ändrad lagstiftning för polisväsendet, utredningen om domstolarnas personuppgiftsbehandling, utredningen om Kustbevakningens personuppgiftsbehandling samt pågående översyner och lagstiftningsarbete i övrigt. Vidare redovisas i avsnitt 7 pågående förhandlingar inom Europeiska unionen om några instrument som är av stor betydelse i detta sammanhang.

4.4 Behandling av personuppgifter inom polisen

4.4.1 Europarådets rekommendation om användningen av personuppgifter inom polissektorn

År 1987 antog Europarådet en rekommendation, No. R (87) 15, om användningen av personuppgifter inom polissektorn. Rekommendationen innehåller regler om skydd för personuppgifter som polisen samlar in, lagrar, använder eller överför med

hjälp av automatiserad behandling i syfte att förhindra och bekämpa brott eller upprätthålla allmän ordning. Endast sådana uppgifter som är nödvändiga för att förhindra en verklig fara eller bekämpa ett visst brott får samlas in, om inte den nationella lagstiftningen tillåter ett mer omfattande uppgiftssamlade. Skilda kategorier av lagrade uppgifter ska så långt som möjligt kunna skiljas från varandra efter graden av riktighet och tillförlitlighet. Det betonas särskilt att uppgifter som grundar sig på fakta ska kunna skiljas från uppgifter som grundar sig på omdömen eller personliga värderingar.

4.4.2 Allmänt om polisens behandling av personuppgifter

Den 1 april 1999 trädde polisdatalagen (1998:622) i kraft (prop. 1997/98:97, bet. 1997/98:JuU20). Den kompletteras av polisdataförordningen (1999:81). Polisdatalagen bygger på personuppgiftslagen och innehåller de särregler som har ansetts nödvändiga i polisens verksamhet.

Polisdatalagen utgör bara en del av lagstiftningen om polisens register. Härutöver finns det bestämmelser om behandling av personuppgifter i lagen (1998:620) om belastningsregister, lagen (1998:621) om misstankeregister, lagen (2000:344) om Schengens informationssystem, lagen (2006:444) om passagerarregister, förordningen (1997:903) om ordningsbotsregister och förordningen (1997:902) om strafförelägganderegister. Många av polisens register förs alljämt, enligt övergångsbestämmelserna till polisdatalagen, med stöd av Datainspektionens tillstånd enligt datalagen.

Polisens register kan i princip delas in i tre kategorier, beroende på vilka bestämmelser som styr behandlingen. Dessa är

- register som förs med stöd av särskilda regler i polisdatalagen eller annan registerlagstiftning,
- register som förs med stöd av personuppgiftslagen och de allmänna bestämmelserna i polisdatalagen, och

- register som enligt övergångsbestämmelserna till polisdatalagen förs med stöd av den numera upphävda datalagen och Datainspektionens tillstånd. För en närmare beskrivning av registerlagstiftningen, se prop. 2007/08:6.

4.4.3 Polisdatalagen

Allmänt om regleringen

Polisdatalagen innehåller både allmänna regler om behandling av personuppgifter i polisiärt arbete och regler om vissa särskilda register. Behandling av personuppgifter som sker med stöd av lagen om belastningsregister, lagen om misstankeregister eller lagen om Schengens informationssystem har undantagits från lagens tillämpningsområde.

Polisdatalagen gäller, utöver personuppgiftslagen, vid behandling av personuppgifter i polisens verksamhet och i polisverksamhet vid Ekobrottsmyndigheten för att

- förebygga brott och andra störningar av den allmänna ordningen och säkerheten,
- övervaka den allmänna ordningen och säkerheten,
- hindra störningar av den allmänna ordningen och säkerheten samt ingripa när något sådant inträffat eller
- bedriva spaning och utredning i fråga om brott som hör under allmänt åtal.

Polisdatalagen innehåller särskilda bestämmelser om vissa register som förs med hjälp av automatiserad behandling. Dessa är kriminalunderrättelseregister, register med uppgifter om DNA-analyser i brottmål, fingeravtrycks- och signalementsregister samt Säkerhetspolisens register (SÄPO-registret).

Polisdatalagen omfattar dock inte all personuppgiftsbehandling inom polismyndigheterna. Uppgiftsbehandling inom exempelvis den hjälpande och stödjande verksamheten och den administrativa verksamheten regleras i personuppgiftslagen. Det finns även andra författningar med bestämmelser om register i polis-

verksamheten, t.ex. 23 § passförordningen (1979:664), men dessa register har andra syften än brottsbekämpning och saknar därför intresse här.

I polisdatalagen finns vissa allmänna bestämmelser, bl.a. om behandling av känsliga personuppgifter (5 §), utlämnande av uppgifter (6–8 §§) samt rättelse och skadestånd (9 §). De allmänna bestämmelserna gäller för all behandling av personuppgifter, dvs. även sådan behandling i register som inte är automatiserad.

Register som regleras särskilt i polisdatalagen

En typ av register som regleras särskilt i polisdatalagen är *kriminalunderrättelseregister*.

Med underrättelseverksamhet förstås i polisdatalagen den polisverksamhet som består i att samla, bearbeta och analysera information för att klarlägga om brottslig verksamhet har utövats, eller kan komma att utövas, och som inte utgör förundersökning enligt 23 kap. rättegångsbalken. Med kriminalunderrättelseverksamhet avses annan underrättelseverksamhet än den som bedrivs av Säkerhetspolisen. Bestämmelserna om kriminalunderrättelseverksamhet finns i 14–21 §§ polisdatalagen.

Automatiserad behandling av personuppgifter får – förutom i kriminalunderrättelseregister – förekomma i s.k. särskilda undersökningar. Sådana får inledas efter särskilt beslut, om det finns anledning att anta att allvarlig brottslighet har utövats eller kan komma att utövas. Undersökningarna har till syfte att ge underlag för beslut om förundersökning eller för beslut om särskilda åtgärder för att förebygga, förhindra eller upptäcka brott. I särskilda undersökningar får även uppgifter om icke misstänkta personer behandlas, men uppgifterna måste förses med upplysning om att personen inte är misstänkt.

Kriminalunderrättelseregister får föras för att ge underlag för beslut om särskilda undersökningar avseende allvarlig brottslig

verksamhet eller för att underlätta tillgången till allmänna uppgifter med anknytning till underrättelseverksamhet.

I lagen anges vilka uppgifter som får finnas i ett kriminalunderrättelseregister. Ett sådant register får innehålla uppgifter som kan hänföras till en enskild person endast om uppgifterna ger anledning att anta att allvarlig brottslig verksamhet har utövats eller kan komma att utövas. Med allvarlig brottslig verksamhet menas verksamhet som innefattar brott för vilket är föreskrivet fängelse i två år eller däröver. Det krävs vidare att den person som avses med uppgifterna skäligen kan misstänkas för att ha utövat eller komma att utöva den allvarliga brottsliga verksamheten. Uppgifter om transportmedel eller varor som kan antas ha samband med allvarlig brottslig verksamhet eller om hjälpmedel som kan ha använts i samband med sådan verksamhet får dock registreras, även om uppgifterna kan hänföras till en enskild person som det inte finns någon misstanke mot. Uppgifterna ska då föras med upplysning om att det inte finns några misstankar mot denne.

Kriminalunderrättelseregister får föras av Rikspolisstyrelsen eller av en polismyndighet. Den myndighet som för registret är personuppgiftsansvarig för behandlingen av personuppgifter i registret.

Register med *uppgifter om DNA-analyser* i brottmål regleras också särskilt. Resultatet av prov för DNA-analys som tagits med stöd av bestämmelserna om kroppsbesiktning i 28 kap. rättegångsbalken får under vissa förutsättningar registreras i register som förs med stöd av polisdatalagen. Bestämmelser om dessa register finns i 22–28 §§ polisdatalagen. Där anges registrens ändamål och vad registren får innehålla.

Med stöd av polisdatalagen förs tre olika register. DNA-registret innehåller DNA-profiler från personer som dömts till annan påföljd än enbart böter. Utredningsregistret innehåller DNA-profiler från personer som är skäligen misstänkta för brott på vilket fängelse kan följa. Spårregistret innehåller uppgifter om DNA-profiler som har tagits fram av spår under utredning av ett brott men som inte kan hänföras till en identifierbar person.

Registren förs hos Statens kriminaltekniska laboratorium men Rikspolisstyrelsen är personuppgiftsansvarig för samtliga register.

Enligt förordningen (1992:824) om fingeravtryck m.m. ska fingeravtryck och fotografi alltid tas av den som häktats. I vissa uppräknade fall ska fingeravtryck och fotografi också tas av den som är anhållen eller av annan. Fingeravtrycket och fotografiet ska skyndsamt sändas till Rikspolisstyrelsen tillsammans med en beskrivning av personen. Styrelsen för ett *fingeravtrycksregister* och ett *signalements- och känneteckensregister*. I 29–31 §§ polisdatalagen regleras fingeravtrycks- och signalementsregister. Paragraferna innehåller bestämmelser om registrens ändamål och om vad registren får innehålla. De nuvarande registren förs dock med tillstånd av Datainspektionen och övergångsbestämmelserna till polisdatalagen.

Säkerhetspolisen ska föra ett särskilt register (*SÄPO-registret*) som har till ändamål att

- underlätta spaning i syfte att förebygga och avslöja brott mot rikets säkerhet,
- underlätta spaning i syfte att bekämpa terrorism, och
- utgöra underlag för registerkontroll enligt säkerhetskyddslagen (1996:627).

SÄPO-registret, som regleras i 32–35 §§ polisdatalagen, är avsett att vara ingången till Säkerhetspolisens hantering av personuppgifter (prop. 1997/98:97 s. 154). Detta innebär att registret endast får innehålla identifieringsuppgifter, uppgifter om grunden för registrering och hänvisning till de ärenden där uppgifter om den registrerade behandlas. Registret fyller dock inte någon operativ funktion i Säkerhetspolisens verksamhet. All behandling av personuppgifter av betydelse för verksamheten sker i andra system (för en närmare beskrivning, se Ds 2007:43 s. 295). Registret förs enbart för att uppfylla kravet i 32 § polisdatalagen om att Säkerhetspolisen ska föra ett sådant register.

4.4.4 Lagen om belastningsregister

I 1 § lagen (1998:620) om belastningsregister föreskrivs att Rikspolisstyrelsen ska föra ett rikstäckande belastningsregister (prop. 1997/98:97, bet. 1997/98:JuU20). Förordningen (1999:1134) om belastningsregister innehåller kompletterande bestämmelser om registret. Alla påföljder för brott ska registreras i belastningsregistret. Registret innehåller för närvarande uppgifter om mellan 800 000 och en miljon personer och omkring 1 200 000 noteringar om påföljder. De allra flesta av dessa noteringar avser bötespåföljder som fastställts genom föreläggande av ordningsbot eller strafföreläggande. Rikspolisstyrelsen är personuppgiftsansvarig för registret.

Belastningsregistret ska, förutom uppgifter om påföljder, innehålla uppgifter om bl.a. den som har ålagts förvandlingsstraff för böter eller vite, den som med tillämpning av 30 kap. 6 § brottsbalken har förklarats fri från påföljd samt om den som har meddelats besöksförbud (3 §). Vissa uppgifter om den som är dömd i utlandet ska också registreras (4 §).

Ändamålet med belastningsregistret är att ge information om sådana belastningsuppgifter som behövs i verksamhet hos polis-, skatte- och tullmyndigheter för att förebygga, upptäcka och utreda brott, hos åklagarmyndigheter för beslut om förundersökning och åtal och vid utfärdande av strafförelägganden samt hos allmänna domstolar för val av påföljd och straffmätning (2 §). Uppgifter i registret får också användas av polismyndigheter och andra myndigheter vid sådan lämplighetsprövning, tillståndsprövning och annan prövning som anges i lag eller förordning samt av enskilda om det är av särskild betydelse i den enskildes verksamhet. I lagen om belastningsregister bemyndigas regeringen att föreskriva att en myndighet får ha direktåtkomst till belastningsregistret.

Lagen och förordningen innehåller tillsammans en uttömmande uppräkningslista av vilka uppgifter som får registreras.

För belastningsregistret gäller enligt 7 kap. 17 § sekretesslagen (1980:100) absolut sekretess och uppgifter får endast lämnas ut

enligt vad som är särskilt föreskrivet. Domstolar och övriga rättsvårdande myndigheter har rätt att få ut de uppgifter som är nödvändiga för att de ska kunna bedriva sin verksamhet (6 §). Vidare har den registrerade alltid rätt att få ut de uppgifter som finns registrerade om honom eller henne (9 §). Även enskilda har rätt att i den utsträckning som regeringen föreskriver få ut uppgifter om andra enskilda från registret bl.a. om det behövs för att pröva fråga om en anställning eller ett uppdrag i en verksamhet som avser vård eller som är av betydelse för att förebygga eller beivra brott (10 §). Vidare får uppgifter i vissa fall lämnas till utländska myndigheter och till myndigheter för statistikändamål.

Såväl myndigheters som enskildas rätt att få information om behandlingen regleras närmare i förordningen.

Uppgifter i belastningsregistret gallras när förutsättningarna för registrering inte längre föreligger, t.ex. om den registrerade blir frikänd efter överklagande eller resning eller om ett beslut om ordningsbot undanröjs. I sådana fall tas registeruppgiften bort så snart beslutet vinner laga kraft. Uppgifter ur belastningsregistret gallras vidare när viss tid förflutit, i regel efter tio år. Bötesdomar gallras redan efter fem år.

Personuppgiftslagens regler om rättelse och skadestånd gäller för behandlingen av personuppgifter i registret (20 §).

4.4.5 Lagen om misstankeregister

Enligt 1 § lagen (1998:621) om misstankeregister ska Rikspolisstyrelsen föra ett rikstäckande register med uppgifter om dem som är skäligen misstänkta för brott (prop. 1997/98:97, bet. 1997/98:JuU20). Förordningen (1999:1135) om misstankeregister innehåller kompletterande bestämmelser om registret. Misstankeregistret omfattar för närvarande cirka 100 000 personer och uppgifter om 225 000 brott. Rikspolisstyrelsen är personuppgiftsansvarig för registret.

Misstankeregistret förs för att underlätta tillgången till sådana uppgifter om skäligen misstanke om brott som behövs i verksamhet hos polis- skatte- och tullmyndigheter för att samordna förundersökningar mot en misstänkt person och för att förebygga, upptäcka och utreda brott samt hos åklagarmyndigheter för beslut om förundersökning och åtal (2 §). Registret får även användas av andra myndigheter som har att utföra lämplighetsprövning, tillståndsprövning eller annan prövning som anges i författning. Slutligen får registret användas för att – i den utsträckning regeringen föreskriver det – till enskild lämna uppgift som är av särskild betydelse i dennes verksamhet.

Misstankeregistret innehåller uppgifter om den som har fyllt 15 år och som är skäligen misstänkt antingen för något brott mot brottsbalken eller för något annat brott för vilket svårare straff än böter är föreskrivet. Uppgifter förs också in om den som är skäligen misstänkt för ett motsvarande brott utomlands, om frågan om lagföring ska avgöras i Sverige. Registret innehåller vidare uppgifter om den mot vilken det har inletts talan om förvandling av böter och om den som begärts överlämnad eller utlämnad för brott.

Lagen och förordningen innehåller tillsammans en uttömmande reglering av vilka uppgifter som får registreras.

De myndigheter för vars räkning registret förs, samt övriga myndigheter i den utsträckning det föreskrivs av regeringen, ska oavsett sekretess ha rätt till uppgifter ur registret (5 §). Uppgifter ur registret ska vidare i viss utsträckning kunna lämnas till myndigheter och organisationer utomlands.

En enskild person har i princip inte någon rätt att få information om huruvida uppgifter om honom eller henne behandlas i registret. Regeringen kan dock i ett enskilt fall medge att uppgifter lämnas ut. Lagen ger också visst utrymme för att lämna uppgifter till enskilda om andra enskilda, om det behövs för att pröva frågor om anställning eller uppdrag inom vården (8 §). De närmare reglerna om detta finns i förordningen.

Uppgifter i misstankeregistret gallras om en förundersökning har avslutats utan att åtal har väckts med anledning av misstan-

ken, om åtal har lagts ned samt när dom eller beslut i anledning av misstanken har vunnit laga kraft (13 §). Ett godkänt strafföreläggande likställs med en dom.

Personuppgiftslagens bestämmelser om rättelse och skadestånd gäller för behandling av uppgifter i misstankeregistret (15 §).

4.4.6 Lagen om Schengens informationssystem

Sverige är sedan senare delen av 1990-talet anslutet till Schengensamarbetet (prop. 1997/98:42, bet. 1997/98:JuU15). Schengensamarbetet bygger på två grundtankar. Den första är den fria rörligheten för personer, i den meningen att personkontroller vid nationsgränserna mellan Schengenstaterna inte ska förekomma. Den andra är att kampen mot internationell kriminalitet och illegal invandring ska stärkas genom samarbetet.

Ett viktigt hjälpmedel i detta samarbete är dataregistret Schengens informationssystem. Informationssystemet består av en nationell enhet för varje Schengenstat och en central teknisk stödfunktion, som är gemensam för Schengenländerna. Lagen (2000:344) om Schengens informationssystem innehåller regler om behandling av personuppgifter i den nationella enheten. Det register som utgör den svenska nationella enheten förs av Rikspolisstyrelsen, som också är personuppgiftsansvarig (1 §). Registret är anslutet till den centrala enheten i Schengens informationssystem. Varje Schengenstats nationella enhet innehåller uppgifter som är identiska med uppgifterna i de övriga ländernas nationella enheter.

Registret är ett hjälpmedel för Schengenstaterna att göra framställningar för att främja samarbete som avser polisiära och rättsliga frågor samt frågor om inresa och uppehållstillstånd (2 §). Det är uppbyggt som ett spanings- och efterlysningshjälpmedel. I informationssystemet kan varje Schengenstat föra in uppgifter om personer eller föremål som är efterlysta eller på annat sätt eftersökta med en begäran om att viss åtgärd ska vidtas när en efterlyst person eller ett efterlyst fordon påträffas. I informa-

tionssystemet finns endast identifieringsuppgifter rörande registrerade personer. De kompletterande uppgifter som behövs för att ett land, som har påträffat en efterlyst person eller ett efterlyst fordon, ska kunna verkställa en begärd åtgärd lämnas över först när det blir aktuellt i varje enskilt fall.

Lagen om Schengens informationssystem reglerar bl.a. vilka framställningar som får föras in i registret (3 §), vilka personuppgifter som får förekomma i registret (4 §) och vem som får använda uppgifter ur det (9 §). Vidare förbjuds användning av uppgifter för annat ändamål än det som uppgiften registrerats för (10 §). I registret förekommer uppgifter om namn, om särskilda bestående fysiska kännetecken, om födelsedatum, födelseort, kön och medborgarskap, om personen är beväpnad, om personen kan förväntas tillgripa våld, om syftet med framställningen samt om begärd åtgärd. Registret innehåller endast uppgifter som har behandlats av behöriga myndigheter i Schengenstaterna, i enlighet med respektive stats nationella lagstiftning.

Rikspolisstyrelsen registrerar endast uppgifter i systemet om behandling av motsvarande slag av uppgifter är tillåten enligt svensk lagstiftning (5 §). Känsliga personuppgifter får inte registreras (7 §). Personuppgiftslagens regel om skadestånd gäller för behandling i registret (13 §). I lagen finns en särskild regel om rättelse av felaktiga uppgifter (12 §).

Uppgifterna i registret gallras senast ett, tre, fem eller tio år efter registreringen. Det tillämpas olika gallringstider för olika slag av uppgifter (11 §).

Bestämmelser om vilka myndigheter som har rätt till uppgifter ur registret och bestämmelser om direktåtkomst finns dels i lagen, dels i förordningen (2000:836) om Schengens informationssystem.

I den mån lagen om Schengens informationssystem inte innehåller avvikande regler, är personuppgiftslagens bestämmelser tillämpliga på registret (se prop. 1999/2000:64 s. 135).

I avsnitt 6.2 redovisas vissa förändringar som är aktuella för Schengens informationssystem.

4.4.7 Lagen om passagerarregister

Lagen (2006:444) om passagerarregister innehåller bestämmelser om behandling av personuppgifter om ankommande passagerare som flygföretag på begäran måste lämna till Rikspolisstyrelsen med stöd av 9 kap. 3 a § utlänningslagen (2005:529). Lagen bygger på ett EG-direktiv, rådets direktiv 2004/82/EG om skyldighet för transportörer att lämna uppgifter om passagerare (prop. 2005/06:129, bet. 2005/06:SfU14). Rikspolisstyrelsen för registret och är personuppgiftsansvarig för detta (1§). Syftet med registret är att underlätta personkontroll vid Sveriges gräns mot sådana stater som inte är medlemmar i Europeiska unionen och som inte heller har träffat avtal om samarbete enligt Schengenkonventionen (4 §).

Om inte annat följer av lagen, eller av föreskrifter som har meddelats med stöd av lagen, tillämpas personuppgiftslagen vid behandlingen av personuppgifter i passagerarregistret (2 §).

I lagen anges uttömmande vilka typer av uppgifter som får registreras. I registret antecknas uppgifter om bl.a. typ av resehandling, medborgarskap, namn, födelsedatum, inreseort samt avgångs- och ankomsttid för transporten (5 §). Huvudregeln är att uppgifterna i registret ska gallras inom 24 timmar. Uppgifterna kan dock få bevaras fram till dess att personkontrollen är avslutad (9 §).

Personuppgiftslagens bestämmelser om rättelse och skadestånd är tillämpliga på registret (10 §).

I avsnitt 7.4 redovisas ett förslag till rambeslut om passageraruppgifter av nu aktuellt slag.

4.4.8 Förordningen om ordningsbotsregister

Rikspolisstyrelsen för, med stöd av förordningen (1997:903) om register över förelägganden av ordningsbot, ett särskilt register för hela landet över alla sådana förelägganden. Registret omfattar även de förelägganden som har beslutats inom Tullverket och

Kustbevakningen. Det utfärdas omkring 250 000 förelägganden av ordningsbot årligen.

Registret får användas som ett stöd för handläggning, uppbörd och underrättelser till myndigheter samt för tillsyn, planering, uppföljning och framställning av statistik (2 §). Registret fungerar således både som ett handläggningsregister och som register för verkställighet av påföljd.

Rikspolisstyrelsen är personuppgiftsansvarig för registret, medan polismyndigheterna, Tullverket och Kustbevakningen är personuppgiftsansvariga för uppgifterna i de ärenden som handläggs hos respektive myndighet (3 §).

Rikspolisstyrelsen och polismyndigheterna får ha direktåtkomst till registret. Tullverket och Kustbevakningen får ha direktåtkomst till uppgifter i de ärenden i registret som handläggs hos respektive myndighet (4 §).

I förordningen anges uttömmande vilka typer av uppgifter registret får innehålla. Till dessa hör bl.a. uppgift om

- fysiska personers namn, adress, personnummer m.m.,
- den brottsliga gärningen,
- förelagd ordningsbot,
- beslagtagna egendom,
- särskild rättsverkan,
- godkännande, samt
- beslut av polisman, åklagare, tulltjänsteman, kustbevakningstjänsteman och domstol.

Förordningen innehåller även regler om sambearbetning av uppgifter, utlämnande av uppgifter i registret, sökbegränsningar och gallring.

Däremot finns ingen regel om rättelse av felaktiga uppgifter eller om skadestånd för otillåten behandling av personuppgifter.

4.4.9 Förordningen om strafförelägganderegister

Förordningen (1997:902) om register över strafförelägganden innehåller bestämmelser om vilka register som får föras i ärenden

om strafförelägganden. I avsnitt 4.5.4 beskrivs regleringen närmare. Rikspolisstyrelsen, som är uppbördsmyndighet, får enligt 4 § föra ett register över uppbörd i ärenden om strafförelägganden. Styrelsen är personuppgiftsansvarig för det registret (7 §), medan Åklagarmyndigheten och Ekobrottsmyndigheten är personuppgiftsansvariga för den behandling som förekommer vid respektive myndighet. Det av Rikspolisstyrelsen förda registret avser verkställighet av påföljd. Enligt 3 § bötesverkställighetsförordningen (1979:197) är styrelsen central uppbördsmyndighet.

I 9 § förordningen om strafförelägganderegister anges vilka uppgifter som registret får innehålla. Det rör sig bl.a. om uppgifter om den misstänkte samt om beslut i ärendet. I 18 § föreskrivs vilka sökbegrepp som får användas vid sökning i uppbördsregistret.

Vidare regleras i 12–15 §§ förordningen i vilken omfattning uppgifter för förs mellan uppbördsregistret och andra register. Det rör sig bl.a. om vissa register som förs av Kronofogdemyndigheten.

4.4.10 Andra register som förs i polisens brottsbekämpande verksamhet

Inom polisen förs, som tidigare nämnts, en rad andra register för brottsbekämpande ändamål än de som regleras särskilt i polisdatalagen eller i någon av de andra särskilda registerförfattningarna. Några av de viktigaste är följande.

Det *allmänna spaningsregistret* (ASP) förs av Rikspolisstyrelsen med stöd av beslut av Datainspektionen och övergångsbestämmelserna till polisdatalagen. ASP innehåller uppgifter om personer som sätts i samband med brottslig verksamhet. Registret kan sägas vara en föregångare till underrättsregistren. Registret innehåller uppgifter om cirka 100 000 personer.

Centrala brottspaningsregistret (CBS) förs av Rikspolisstyrelsen. Det anses numera tillhöra de register som förs med stöd av övergångsbestämmelserna till polisdatalagen. CBS innehåller

uppgifter om anmälda brott av allvarligare slag. Registret innehåller noteringar om cirka 129 000 brott. Det används framför allt för att söka efter likartade brott eller brott som har begåtts av samma person.

Beslags- och analysregister (BAR) förs av Rikspolisstyrelsen och polismyndigheterna med stöd av tillstånd från Datainspektionen och övergångsbestämmelserna till polisdatalagen. BAR har två ändamål; dels att ge upplysningar om modus operandi och profiler av strategisk betydelse för nationell och internationell narkotikabekämpning, dels att rapportera beslagtagna narkotika.

Finanspolisens analys- och spaningsregister förs med stöd av polisdatalagen och personuppgiftslagen. Registret har till stor del underrättelsekaraktär men används också som diarium för Finanspolisen. Registret innehåller uppgifter om penningtvätt.

Rikspolisstyrelsen för, efter beslut av regeringen, ett *Digitalt referensbibliotek över barnpornografiska framställningar*. Syftet med registret är att kunna analysera barnpornografiska framställningar i brottsutredningar och innehållet består av sådana bilder som tagits i beslag. Registret förs med stöd av polisdatalagen och personuppgiftslagen.

Personefterlysningsregistret, som tillsammans med U-boken utgör det s.k. EPU-systemet, förs med stöd av tillstånd från Datainspektionen och övergångsbestämmelserna till polisdatalagen. Syftet med EPU-systemet är i korthet att

- föra register över efterlysta personer,
- sammanställa och sprida uppgifter om utvisnings- och avvisningsbeslut, om beslutet är förenat med återreseförbud samt
- utgöra underlag för passkontroll och beslut i passärenden.

Godsregistret består av två delar, godsregistret och bevakningsregistret. Det förra innehåller uppgifter om gods som stulits, förkommit eller tagits om hand t.ex. genom beslag. I bevakningsregistret registreras uppgifter om gods som tagits i beslag och som inte har återfunnits i godsregistret men som förväntas komma att bli registrerat som stulet eller förkommet. Godsregistret förs

med stöd av beslut av Datainspektionen och övergångsbestämmelserna till polisdatalagen.

Efterlysningssystemet för fordon innehåller uppgifter om efterlysta fordon och förs i syfte att underlätta spaningen efter fordonen. Det förs med stöd av tillstånd av Datainspektionen och övergångsbestämmelserna till polisdatalagen.

En närmare beskrivning av de nu nämnda registren och vissa andra register som förs inom polisen finns i Ds 2007:43, bilaga 6 (s. 595 ff.).

4.4.11 Register med annat primärt ändamål

Inom polisen förs också vissa register där brottsbekämpning endast är ett av flera ändamål, nämligen vapenregistren. I 2 kap. vapenlagen (1996:67) finns bestämmelser om lokala och centrala vapenregister. Varje polismyndighet för ett lokalt vapenregister över tillståndspliktiga vapeninnehav. Rikspolisstyrelsen för separata centrala register över vapeninnehavare, vapen och vapenhandlare. De centrala vapenregistren får av säkerhetsskäl inte samköras med varandra.

Enligt 2 kap. 20 § vapenlagen ska vapenregistren ha till ändamål att dels ge information om sådan uppgifter som behövs för att förebygga, upptäcka och utreda brott med anknytning till skjutvapen, dels att underlätta handläggningen av frågor om tillstånd enligt vapenlagen. I förarbetena framhålls den stora betydelse centrala vapenregister har för polisarbetet. Det gäller både det förebyggande arbetet och arbetet med att utreda brott (prop. 1998/99:36 s. 14 f. och 20).

Vapeninnehavarregistret innehåller uppgifter om namn, personnummer och adress på de personer som har meddelats tillstånd att inneha skjutvapen eller ammunition enligt vapenlagen samt uppgift om polismyndighet och polisområde.

Det centrala *vapenregistret* innehåller uppgifter om vapen som exempelvis tillstandsnummer, tillståndstyp, tillståndets giltighetstid, vapentyp, fabrikat, modell, kaliber, tillverkningsnummer

m.m. Vidare innehåller det uppgifter om sådana vapen som upphittats eller anmälts stulna eller försvunna.

I *vapenhandlarregistret* registreras bl.a. uppgifter om organisationsnummer, namn, adress och tillståndsnummer på de fysiska eller juridiska personer som har tillstånd att driva handel med skjutvapen.

Polisdatalagens allmänna bestämmelser är tillämpliga på vapenregistren (se prop. 1998/99:36 s. 20). Personuppgiftslagen bestämmelser om rättelse och om skadestånd gäller för vapenregistren genom en hänvisning i 2 kap. 21 § vapenlagen.

4.5 Andra myndigheters behandling av personuppgifter för brottsbekämpning

4.5.1 Tullverket

Tullbrottsdatabasen

Den 1 december 2005 trädde lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet i kraft (prop. 2004/05:164, bet. 2005/06:SkU3). Lagen behandlar i stort sett samma frågor som polisdatalagen men är uppbyggd på lite annorlunda sätt. Lagen innehåller dels allmänna regler om behandling av personuppgifter i tullens brottsbekämpande arbete, dels bestämmelser om en särskild databas, tullbrottsdatabasen (3 §). Tullverket är personuppgiftsansvarig för behandling enligt lagen, om inte annat föreskrivs (10 §).

Lagen gäller endast om behandlingen är helt eller delvis automatiserad eller om personuppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter (1 §). Lagen tillämpas även i viss utsträckning på behandling av uppgifter om juridiska personer.

Till skillnad från flertalet andra författningar om behandling av personuppgifter gäller denna i stället för personuppgiftslagen

(5 §), men vissa bestämmelser i personuppgiftslagen är tillämpliga, vilket framgår av 6 §.

I 7 § anges uttömmande för vilka ändamål personuppgifter får behandlas. Personuppgifter får behandlas i Tullverkets brottsbekämpande verksamhet om det behövs för att

- förhindra eller upptäcka brottslig verksamhet,
- utreda eller beivra visst brott, eller
- fullgöra det arbete som Tullverket är skyldigt att utföra enligt lagen (2000:1219) om internationellt tullsamarbete.

Vidare får sådana uppgifter behandlas när det är nödvändigt för att tillhandahålla information till andra svenska brottsbekämpande myndigheter (8 §). Dessutom får uppgifter lämnas ut till riksdagen och regeringen samt, i den utsträckning uppgiftsskyldighet följer av lag eller förordning, till andra (9 §).

Sådana känsliga personuppgifter som avses i 13 § personuppgiftslagen (se avsnitt 4.2.5) får inte behandlas enbart på den grunden. Om uppgifter om en person behandlas på annan grund får de dock kompletteras med känsliga personuppgifter när det är absolut nödvändigt för syftet med behandlingen (11 §).

I 12–15 §§ anges de närmare förutsättningarna för behandling av uppgifter för de tre huvudsyften som anges i 7 §.

För ändamålet att förhindra eller upptäcka brottslig verksamhet får enligt 12 § uppgifter om en person behandlas i följande fall.

- Om uppgifterna dels ger anledning att anta att brottslig verksamhet, som innefattar brott för vilket är föreskrivet fängelse i minst två år har utövats eller kan komma att utövas, eller som innefattar andra brott, om verksamheten sker systematiskt, dels gör att personen skäligen kan misstänkas för verksamheten i fråga.
- Uppgifter som inte direkt kan hänföras till en person, om uppgifterna avser sådana transportmedel, varor eller hjälpmedel som kan antas ha samband med sådan verksamhet som nyss sagts.
- Om uppgifterna avser en person som, utan att vara skäligen misstänkt, kan antas ha samband med sådan verksamhet.

Dessutom får uppgifter om passagerare, importörer, exportörer och transportörer samt varor och transportmedel behandlas i syfte att förhindra eller upptäcka brottslig verksamhet (13 §).

För ändamålet att utreda och beivra brott får uppgifter om den som kan misstänkas för brottet och om andra personer behandlas när det behövs för att utreda eller beivra brottet (14 §).

Uppgifter om en person som inte är misstänkt för brott ska föras med en särskild upplysning om detta, om det inte på annat sätt klart framgår att personen i fråga inte är misstänkt. Motsvarande gäller för uppgifter om en person som inte skäligen kan misstänkas ha utövat eller komma att utöva brottslig verksamhet. Uppgifter om en person som kan ha samband med brottslig verksamhet ska föras med upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak (16 §).

I 19 § anges i detalj vilka typer av personuppgifter som får behandlas i tullbrottsdatabasen och i 20–22§ anges vilka sökbegrepp som får användas. Inom ramen för tullbrottsdatabasen får särskilda underrättsregister inrättas enligt 9 § förordningen (2005:971) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet.

Lagen innehåller också regler om bl.a. uppgiftsskyldighet (23 och 24 §§), utlämnande av uppgifter på medium för automatiserad behandling (25 §), direktåtkomst (26 §), gallring (27 och 28 §§), information till den registrerade (29 §) och överklagande (30 §).

I förordningen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet finns kompletterande bestämmelser, bl.a. om direktåtkomst till tullbrottsdatabasen.

Tullinformationssystemet

Tullinformationssystemet (TIS) består av två komponenter. Den ena bygger på Europeiska rådets förordning (EG) nr 515/97 av den 13 mars 1997 om ömsesidigt bistånd mellan medlemsstaters administrativa myndigheter och om samarbete mellan dessa och

kommissionen för att säkerställa en korrekt tillämpning av tull- och jordbrukslagstiftningen, som reglerar frågor inom första pelaren (TIS I). Den andra har sin rättsliga grund i Konventionen av den 26 juli 1995, som utarbetats på grundval av artikel K 3 i Fördraget om Europeiska unionen, om användning av informationsteknologi för tulländamål (TIS-konventionen) och reglerar samarbetet inom tredje pelaren (TIS III). Tullinformationssystemet utgör ett samlingsbegrepp för två från varandra logiskt skilda databaser, TIS I och TIS III. Det är enbart den sistnämnda delen av systemet som är av intresse här och som berörs i det följande.

Syftet med systemet är att stärka samarbetet mellan främst tullmyndigheterna inom Europeiska unionen, men även mellan andra brottsbekämpande myndigheter, om dessa har till uppgift att bekämpa illegal handel med varor och brott mot nationell lag som begränsar den fria rörligheten av varor. Det närmare ändamålet är att bistå med att förebygga, utreda och lagföra grova överträdelse av nationella lagar genom att påskynda informationsspridningen och därmed öka effektiviteten hos tullmyndigheterna i medlemsstaterna.

Tullinformationssystemet skall endast innehålla sådana uppgifter som är nödvändiga för att uppnå nyssnämnda syfte, inkluderande uppgifter som rör enskilda personer, och inom kategorierna varor, transportmedel, företag, personer, utvecklingen vad avser bedrägeri samt tillgång till sakkunskap. Uppgifterna får endast registreras i systemet under förutsättning att en särskild åtgärd begärs (observation och rapportering, diskret övervakning eller särskild kontroll). Konventionen återges i prop. 1997/98:11 s. 124 ff.

Endast de nationella myndigheter som utses har direkt tillgång till TIS; jfr förordningen (1998:64) om tillämpning av Europeiska unionens tullinformationssystem.

TIS-konventionen har byggts ut med bl.a. ett protokoll som behandlar inrättandet av ett register för identifiering av tullutredningar kallat FIDE (fichier d'identification des dossiers d'enquêtes douanière). Syftet med registret är att underlätta för

tullmyndigheterna (och andra behöriga myndigheter) att identifiera pågående och avslutade tullutredningar avseende grova överträdelser av nationell lagstiftning i andra medlemsstater. I FIDE finns bland annat information om vilken enhet i en medlemsstat som är ansvarig för en viss utredning. Vidare finns information om den person eller det företag som är eller har varit föremål för utredningen, vilket område som utredningen gäller samt kontaktinformation. FIDE medger inget direkt informationsutbyte mellan de behöriga myndigheterna. Om en myndighet genom att söka i registret påträffar uppgifter som verkar vara av intresse ska de existerande instrumenten för informationsutbyte användas, till exempel Neapel II-konventionen. Protokollet om FIDE trädde i kraft 10 oktober 2007 och systemet förväntas vara i drift våren 2008.

Tullverket är registeransvarigt för TIS i Sverige. Datainspektionen är svensk tillsynsmyndighet för skydd av uppgifter i TIS enligt artikel 37 i rådsförordningen.

4.5.2 Kustbevakningen

Kustbevakningens behandling av personuppgifter regleras av personuppgiftslagen och förordningen (2003:188) om behandling av personuppgifter inom Kustbevakningen. Förordningen är uppbyggd på ungefär samma sätt som motsvarande författning för Tullverket. Kustbevakningen är personuppgiftsansvarig för behandlingen (8 §).

Förordningen tillämpas på personuppgiftsbehandling i

- brottsbekämpning,
- kontroll och tillsyn, samt
- ärenden om vattenföroreningsavgift (1 §).

Förordningen tillämpas även i viss utsträckning på behandling av uppgifter om juridiska personer.

I det följande redovisas endast de regler som gäller för den brottsbekämpande verksamheten.

I förordningen finns dels allmänna regler om behandling av personuppgifter i Kustbevakningen brottsbekämpande arbete, dels bestämmelser om ett särskilt register för den verksamhet som förordningen omfattar, kustbevakningsdatabasen.

Förordningen gäller utöver personuppgiftslagen (1 §). Den innehåller ingen hänvisning till tillämpliga bestämmelser i den lagen, men det slås fast att de begrepp som används i förordningen har samma betydelse som i personuppgiftslagen (3 §).

I den brottsbekämpande verksamheten får personuppgifter behandlas om det är nödvändigt för att förhindra eller upptäcka brottslig verksamhet som innefattar brott mot vilka Kustbevakningen har att ingripa, eller för att utreda sådana brott (4 §).

Sådana känsliga personuppgifter som avses i 13 § personuppgiftslagen (se avsnitt 4.2.5) får inte behandlas enbart på den grunden. Om uppgifter om en person behandlas på annan grund får de dock kompletteras med känsliga personuppgifter, om det är oundgängligen nödvändigt för syftet med behandlingen (9 §).

I förordningen skiljer man mellan uppgifter som används gemensamt i verksamheten (kustbevakningsdatabasen) och uppgifter som endast enskilda eller begränsade grupper av tjänstemän har tillgång till (11 §). Behandlingen av uppgifter i kustbevakningsdatabasen omgärdas av särskilda regler när det gäller de personer om vilka uppgifter får behandlas, vilka uppgifter som får förekomma och sökbegränsningar.

I förordningen regleras vidare vilka myndigheter som kan få åtkomst till kustbevakningsdatabasen och i vilken utsträckning det får ske genom direktåtkomst. Det finns också bl.a. bestämmelser om sökning och gallring.

Personuppgiftslagens bestämmelser om rättelse och skadestånd tillämpas på behandling enligt förordningen (23 §).

4.5.3 Skatteverket

I lagen (1999:90) om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar (prop. 1998:99:34, bet.

1998/99:SkU9) och förordningen (1999:105) om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar regleras behandlingen av personuppgifter i verkets brottsbekämpande verksamhet. Lagen – som gäller dels för spaning och utredning av brott, dels för att förebygga brott – är uppbyggd med polisdatalagen som förebild och gäller utöver personuppgiftslagen.

Skatteverkets medverkan i brottsbekämpande verksamhet omfattar endast de brott som anges i 1 § lagen (1997:1024) om Skatteverkets medverkan i brottsutredningar, dvs. brott mot

- skattebrottslagen (1971:69),
- 30 kap. 1 § första stycket 4 aktiebolagslagen (2005:551),
- 11 § tredje stycket lagen (1967:531) om tryggande av pensionsutfästelse m.m.,
- folkbokföringslagen (1991:481),
- 11 kap. 5 § brottsbalken, samt
- lagen (1986:436) om näringsförbud.

Eftersom Skatteverket får medverka vid förundersökning i fråga om andra brott, om åklagaren finner särskilda skäl för det, omfattar tillämpningsområdet även sådana brott.

Skatteverket är personuppgiftsansvarig för den behandling av uppgifter som sker med stöd av lagen (3 §).

Lagen, som enligt 1 § gäller utöver personuppgiftslagen, gäller endast om behandlingen är helt eller delvis automatiserad eller om personuppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter.

I lagen definieras begreppen underrättelseverksamhet, allvarlig brottslig verksamhet och särskild undersökning på samma sätt som i polisdatalagen (2 §). De begrepp som används i personuppgiftslagen har motsvarande betydelse i den nu aktuella lagen.

I lagen regleras en särskild typ av register, underrättelseregister. Regleringen har utformats med polisdatalagen som förebild. Underrättelseregister får föras för två ändamål:

- att ge underlag för beslut om särskilda undersökningar avseende allvarlig brottslighet, eller

- att underlätta tillgången till allmänna uppgifter med anknytning till underrättelseverksamhet.

Ett underrättelseregister får innehålla uppgifter som kan hänföras till en enskild person endast om uppgifterna ger anledning att anta att allvarlig brottslighet utövats eller kan komma att utövas och den som avses med uppgifterna skäligen kan misstänkas för denna verksamhet (9 §). Dessutom får uppgifter om transportmedel eller varor som kan antas ha samband med allvarlig brottslig verksamhet eller hjälpmedel som kan antas ha använts vid sådan brottslighet registreras, även om uppgifterna kan hänföras till en enskild person som det inte finns någon misstanke mot. Då ska emellertid uppgifterna förse med upplysning om att personen inte är misstänkt.

Lagen innehåller också en uttömmande reglering av vilka typer av personuppgifter som får förekomma i underrättelseregister (10 §).

Sådana känsliga personuppgifter som avses i 13 § personuppgiftslagen (se avsnitt 4.2.5) får inte behandlas enbart på den grunden. Om uppgifter om en person behandlas på annan grund får de kompletteras med känsliga personuppgifter, om det är absolut nödvändigt för syftet med behandlingen. Känsliga personuppgifter får dock aldrig behandlas i underrättelseverksamhet (4 §).

Lagen innehåller också uppgifter om utlämnande av uppgifter (5–7 §§) och om gallring (15 §).

Bestämmelserna i personuppgiftslagen om rättelse och skadestånd gäller vid behandling av personuppgifter enligt lagen (16 §). Skatteverkets beslut i fråga om rättelse får överklagas (17 §).

4.5.4 Åklagarväsendet

Förordningen om behandling av personuppgifter inom åklagarväsendet

Förordningen (2006:937) om behandling av personuppgifter inom åklagarväsendet gäller utöver personuppgiftslagen (1 §). Den är tillämplig på Åklagarmyndighetens och Ekobrottsmyndighetens åklagarverksamhet, om behandlingen av personuppgifter är helt eller delvis automatiserad eller om uppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter. Sådan behandling av personuppgifter som regleras i förordningen om register över strafförelägganden har undantagits från tillämpningsområdet.

Åklagarmyndigheten och Ekobrottsmyndigheten är enligt 6 § personuppgiftsansvariga för den personuppgiftsbehandling som förekommer vid respektive myndighet.

Inom åklagarväsendet förs en ärendedatabas, vars ändamål och innehåll regleras i förordningen. Direktåtkomsten till uppgifter i databasen begränsas till vad en åklagare eller annan anställd inom åklagarväsendet behöver för att utföra sina arbetsuppgifter.

I 7–9 §§ anges uttömmande vilken behandling av personuppgifter som är tillåten. Huvudregeln är att uppgifter om den som kan misstänkas för brott och om andra personer får behandlas, när det behövs för att en åklagare ska kunna utföra de uppgifter som enligt rättegångsbalken eller annan författning ankommer på åklagare (7 §). Vidare får personuppgifter behandlas för tillsyn, planering, uppföljning eller framställning av statistik. Dessutom får uppgifter behandlas när det är nödvändigt för att tillhandahålla information som behövs i författningsreglerad verksamhet hos en brottsbekämpande eller brottsbeivrande myndighet (8 §) eller för att lämna uppgifter till andra, om uppgiftsskyldighet följer av lag eller förordning.

Sådana känsliga personuppgifter som avses i 13 § personuppgiftslagen (se avsnitt 4.2.5) får inte behandlas enbart på den grunden. Om uppgifterna finns i en handling som kommit in till

myndigheten får de dock behandlas. Om uppgifter om en person behandlas på annan grund får de kompletteras med känsliga personuppgifter, om det är absolut nödvändigt för syftet med behandlingen (10 §).

I 13 § anges vilka personuppgifter som ärendedatabasen får innehålla om fysiska och juridiska personer. Det rör sig bl.a. om uppgifter som behövs för kommunikation med personen, uppgifter om en fysisk eller juridisk persons ställning och koppling till andra personer i ett ärende samt uppgifter om fysiska personerna personliga och ekonomiska förhållanden, om juridiska personers ekonomiska förhållanden, uppgifter om brottshjälpmedel och transportmedel samt om beslut, händelser och åtgärder i ett ärende.

Förordningen reglerar också i 14–16 §§ vilka sökbegrepp som får användas vid sökning i ärendedatabasen samt utlämnande av uppgifter (17 och 18 §§) och gallring (21 §).

Bestämmelserna i personuppgiftslagen om rättelse och skadestånd gäller vid behandling av personuppgifter enligt förordningen (19 §).

Förordningen omfattas av den översyn av behandlingen av personuppgifter inom åklagarväsendet som nämns i avsnitt 6.8.

Strafförelägganderegister

Förordningen (1997:902) om register över strafförelägganden innehåller, som tidigare nämnts, bestämmelser om vilka register som får föras i ärenden om strafförelägganden. Det centrala strafförelägganderegistret får användas för handläggning av ärenden om strafföreläggande och för uppgiftslämnande enligt strafföreläggandekungörelsen (1970:60). Omkring 40 000 strafförelägganden godkänns årligen.

Åklagarmyndigheten får enligt 3 § förordningen föra ett centralt register för strafförelägganden. Vidare får Åklagarmyndigheten, Ekobrottsmyndigheten och Tullverket enligt 2 § föra lokala register över strafförelägganden. Åklagarmyndigheten,

Ekobrottsmyndigheten och Tullverket är personuppgiftsansvariga för de register som förs vid respektive myndighet.

I 9 § finns bestämmelser om vilka uppgifter som registren får innehålla. Det rör sig såvitt gäller strafförelägganderegister bl.a. om uppgifter om den misstänkte och om målsäganden samt om gärningen, påföljden, beslut i ärendet och underrättelser. I 17 och 18 §§ anges vilka sökbegrepp som får användas vid sökning i registren.

Vidare anges i 12–15 §§ förordningen i vilken omfattning uppgifter för föras mellan strafförelägganderegister och andra register. Det rör sig bl.a. om rapportering till misstankeregistret och belastningsregistret.

Förordningen innehåller inga bestämmelser om rättelse av felaktiga uppgifter eller om skadestånd för otillåten behandling av personuppgifter.

Förordningen omfattas av den översyn av behandlingen av personuppgifter inom åklagarväsendet som nämns i avsnitt 6.8.

4.6 Lagstiftning om behandling av personuppgifter inom andra verksamhetsområden som berörs av rambeslutet

4.6.1 Allmänna utgångspunkter

Eftersom tillämpningsområdet för rambeslutet även omfattar internationellt rättsligt samarbete, som innefattar bl.a. rättslig hjälp, och verkställighet av straffrättsliga påföljder sträcker det sig utanför de brottsbekämpande myndigheternas krets. Rättsligt samarbete hanteras till viss del av åklagarväsendet. Domstolsväsendet berörs också. Enligt vissa författningar ska nämligen domstol pröva frågor om rättslig hjälp eller meddela beslut som krävs för handläggningen av exempelvis överlämnanden enligt den europeiska arresteringsordern eller ärenden om rättslig hjälp. Vidare ska domstol besluta i vissa frågor som rör övertagande av

straffverkställighet. På verkställighetsstadiet berörs framför allt kriminalvården.

Det straffrättsliga samarbetet äger rum genom direkt kommunikation mellan berörda myndigheter eller via respektive stats centralmyndighet. Centralmyndigheten för rättslig hjälp i brottmål (som ingår i Regeringskansliet) mottar och överlämnar framställningar om rättslig hjälp i de fall där direktkommunikation inte får eller kan användas. Myndighetens uppgift är främst att fungera som en ”brevlåda” och mellanhand mellan myndigheter i andra länder och svenska myndigheter. Centralmyndigheten hanterar också frågor som kräver beslut av regeringen. Utvecklingen inom Europeiska unionen går mot lösningar som bygger på kommunikation direkt mellan berörda myndigheter såsom åklagare, domstolar och de myndigheter som svarar för verkställighet av straffrättsliga påföljder. Centralmyndighetens roll när det gäller internationellt rättsligt samarbete mellan medlemsstaterna i Europeiska unionen kommer därför i stort sett att försvinna.

4.6.2 Kriminalvården

Allmänt om regleringen

Kriminalvårdens behandling av personuppgifter regleras i lagen (2001:617) om behandling av personuppgifter inom kriminalvården (prop. 2000/01:126, bet. 2000/01:JuU31) och förordningen (2001:682) om behandling av personuppgifter inom kriminalvården. Regleringen gäller för samtliga myndigheter inom kriminalvården, således inte bara för myndigheten Kriminalvården utan även för övervakningsnämnderna och Kriminalvårdsnämnden.

Lagen innehåller endast övergripande bestämmelser för behandlingen, medan förordningen bl.a. innehåller bestämmelser om de register som ska föras inom kriminalvården (centrala kriminalvårdsregistret och säkerhetsregistret) och detaljerade regler

om vilka typer av uppgifter som får behandlas beträffande olika personkategorier.

Lagen innehåller vissa särbestämmelser i förhållande till personuppgiftslagen, som i övrigt gäller för kriminalvårdens verksamhet (2 §).

Lagen gäller vid behandling av personuppgifter i fråga om personer som

- är föremål för personutredning,
- är häktade,
- är dömda till fängelse, skyddstillsyn eller villkorlig dom med föreskrift om samhällstjänst, eller som på grund av utländsk dom ska verkställa en sådan påföljd i Sverige,
- har ålagts förvandlingsstraff för böter eller vite,
- på annan grund är intagna i häkte eller kriminalvårdsanstalt, eller
- som annars transporteras av kriminalvårdens transporttjänst.
- Enligt 3 § får personuppgifter behandlas bara om det är nödvändigt för att
- kriminalvården ska kunna fullgöra sin uppgifter i enlighet med lag eller förordning,
- underlätta tillgången till sådana uppgifter om verkställighet av påföljd eller häktning som rättsväsendets myndigheter behöver, eller
- upprätthålla säkerheten och förebygga brott under häktning, verkställighet av påföljd, intagning av annat skäl eller transport.

Kriminalvården är personuppgiftsansvarig för behandlingen (4 §). Bara de personer som behöver det på grund av sina arbetsuppgifter får ha direktåtkomst till uppgifter (6 §).

Sådana känsliga uppgifter som avses i 13 § personuppgiftslagen (se avsnitt 4.2.5) får inte behandlas enbart på den grunden. Om uppgifter om en person behandlas på annan grund får uppgifterna kompletteras med sådana uppgifter, om det är oundgängligen nödvändigt för syftet med behandlingen. Sådana upp-

gifter får inte användas som sökbegrepp, om inte regeringen har föreskrivit det.

Reglerna i personuppgiftslagen om rättelse och skadestånd gäller vid behandling av personuppgifter enligt lagen eller föreskrifter som har meddelats med stöd av lagen (8 §).

Ett beslut om rättelse eller om information enligt 26 § personuppgiftslagen får överklagas hos allmän förvaltningsdomstol (12 §). Beslutet ska dock först omprövas av Kriminalvården (13–15 §§).

Register som regleras särskilt

Det *centrala kriminalvårdsregistret* regleras i 34–36 §§ förordningen. Ändamålet med registret är dels att myndigheten ska kunna fullgöra sina författningsenliga uppgifter, dels att underlätta tillgången till sådana uppgifter om verkställighet av påföljd som rättsväsendets myndigheter behöver. Registret omfattar endast personer som har dömts till fängelse, skyddstillsyn eller villkorlig dom med föreskrift om samhällstjänst, eller har ålagts förvandlingsstraff för böter eller vite, eller som på grund av utländsk dom ska verkställa en sådan påföljd i Sverige. I 36 § förordningen åläggs Rikspolisstyrelsen att lämna uppgifter om domar med nyss nämnda påföljder samt om överklaganden, inhibition och laga kraft beträffande sådana domar. Regeringskansliet ska lämna uppgifter om beslut i nådeärenden samt vissa beslut enligt utlänningslagen. I 37 § förordningen regleras vilka myndigheter som har rätt att få uppgifter ur registret. Till dessa hör bl.a. myndigheter inom åklagarväsendet och polisväsendet samt domstolar.

Säkerhetsregistret regleras i 39–41 samt 43–46 §§ förordningen.

Ändamålet med registret är att upprätthålla ordningen och att förebygga brott. Registret omfattar endast personer som är häktade eller intagna i vissa kriminalvårdsanstalter för att avtjäna fängelsestraff eller som ska verkställa en utländsk sådan påföljd och som

- är eller tidigare har varit placerade på säkerhetsavdelning inom kriminalvården,
- i häkte eller under verkställighet av ett fängelsestraff gjort sig skyldiga till allvarligt hot eller våld mot personal eller mot andra intagna,
- i häkte eller under verkställighet av ett fängelsestraff har be-
fattet sig med narkotika som inte varit avsedd för eget bruk,
- rymt eller fritagits från häkte eller slutet kriminalvårds-
anstalt eller som förberett rymning eller fritagning eller
gjort försök därtill, eller
- misstänks för att i häkte eller under verkställighet av ett
fängelsestraff ha deltagit i nätverk som bidrar till allvarliga
ordningsstörningar eller brottslig verksamhet (39 §
förordningen).

Dessutom får registret innehålla uppgifter om sådana häktade eller intagna som det finns särskild anledning att anta att de under häktnings- eller anstaltstiden bl.a. kommer att utöva all-
varlig brottslig verksamhet, göra sig skyldiga till vissa typer av
brott eller förbereda rymning eller fritagning.

Förordningen innehåller också regler om de journaler som ska
föras över verkställigheten (10, 16, 22 och 26 §§).

Vid överflyttning av verkställighet av påföljd till en annan stat
får bl.a. sådana journaler lämnas ut till den myndighet i den andra
staten som är ansvarig för verkställigheten (48 § förordningen).

4.6.3 Domstolsväsendet

Behandlingen av personuppgifter inom domstolsväsendet regle-
ras, såvitt är av intresse i detta sammanhang, i tre olika förord-
ningar. En av dem innehåller bestämmelser om behandlingen i
allmän domstol och de två andra bestämmelser om behandlingen
i förvaltningsdomstol.

Förordningen (2001:639) om registrering m.m. vid allmänna
domstolar med hjälp av automatiserad behandling gäller vid
automatiserad behandling av personuppgifter i Högsta domsto-

lens, hovrätternas och tingsrätternas rättskipande och rättsvårdande verksamhet. Vid de allmänna förvaltningsdomstolarna tillämpas förordningen (2001:641) om registerföring m.m. vid Regeringsrätten och kammarrätterna med hjälp av automatiserad behandling respektive förordningen (2001:640) om registerföring vid länsrätt med hjälp av automatiserad behandling.

De tre förordningarna är uppbyggda på samma sätt och innehåller i stor utsträckning likalydande bestämmelser. Redogörelsen i det följande omfattar således alla tre förordningarna, om inte annat sägs.

Förordningarna gäller utöver personuppgiftslagen, som således i övrigt gäller för personuppgiftsbehandlingen inom domstolsväsendet. En domstol är personuppgiftsansvarig för den behandling som domstolen utför.

Förordningarna innehåller bestämmelser om två typer av register, nämligen verksamhetsregister och rättsfallsregister.

Domstolarna får föra *verksamhetsregister*, vilkas övergripande ändamål är att vara ett hjälpmedel vid handläggningen av mål och ärenden. Enligt förordningarna får registren användas för

- handläggning av mål och ärenden,
- planering, uppföljning och utvärdering av verksamheten, och
- framställning av statistik.

För andra domstolar än länsrätter finns ett fjärde ändamål, nämligen att fullgöra författningssenlig underrättelseskyldighet.

Ett verksamhetsregister får endast innehålla de uppgifter som anges i en detaljerad uppräkningsbilaga till respektive förordning. Det rör sig om uppgifter om bl.a. mål eller ärenden, om parter och andra aktörer, om personer som ska höras eller yttra sig, om förhandling, om handläggningen i övrigt och om rättegångskostnader.

Vid angivande av vad saken gäller (ärendemening) får sådana känsliga personuppgifter som anges i 13 § personuppgiftslagen (se avsnitt 4.2.5) och uppgifter om lagöverträdelse m.m. som anges i 21 § personuppgiftslagen behandlas endast om det är

nödvärdigt för att saken ska kunna återges på ett ändamålsenligt sätt. I övrigt får sådana uppgifter behandlas endast om uppgifterna har lämnats i ett mål eller ärende eller om de behövs för handläggningen av målet eller ärendet. Känsliga personuppgifter får inte användas som sökbegrepp.

Samtliga förordningar innehåller regler om gallring i verksamhetsregister.

Domstolarna får vidare föra *rättsfallsregister* för återsökning av vägledande avgöranden, rättsutredningar och liknande rättslig information. Ett sådant rättsfallsregister får endast innehålla de uppgifter som anges i en detaljerad uppräkningsbilaga till respektive förordning. Det rör sig om uppgifter om bl.a. mål- och ärendenummer, avgörandenummer, avgörandedatum, sökord och fullföljd. Personuppgiftslagens regler om gallring tillämpas på registren.

Vid sidan av behandlingen i register innehåller förordningarna också bestämmelser om att domstolarna får behandla personuppgifter automatiserat i löpande text, ljudupptagningar eller ljud- och bildupptagningar. Regleringen har betydelse bl.a. för ordbehandling, e-postfunktioner och digitala ljud- och bildupptagningar. Personuppgifter som behandlas i löpande text eller i ljud- och bildupptagningar bevaras eller gallras enligt bestämmelserna i personuppgiftslagen.

Bestämmelserna i personuppgiftslagen om rättelse och skadestånd gäller vid behandling av personuppgifter enligt förordningarna.

Förordningarna innehåller särskilda regler om överklagande. Beslut i de högsta domstolarna kan inte överklagas. Övriga domstolars beslut överklagas till närmast högre instans inom domstolväsendet.

4.7 Tillsyn över personuppgiftsbehandling

4.7.1 Datainspektionen

Datainspektionen är enligt 2 § personuppgiftsförordningen tillsynsmyndighet enligt personuppgiftslagen. Enligt 2 § förordningen (2007:975) med instruktion för Datainspektionen är inspektionen likaså tillsynsmyndighet enligt dataskyddsdirektivet. Datainspektionen är vidare enligt 4 § instruktionen nationell tillsynsmyndighet enligt

- artikel 23 i Europokonventionen,
- artikel 114 i Schengenkonventionen, och
- artikel 17 i konventionen om användning av informationsteknologi för tulländamål.

Datainspektionens befogenheter i egenskap av tillsynsmyndighet regleras såvitt gäller personuppgiftslagen och dataskyddsdirektivet i personuppgiftslagen. Eftersom de flesta författningar om personuppgiftsbehandling gäller vid sidan av personuppgiftslagen innebär detta att Datainspektionen är tillsynsmyndighet. Datainspektionen anses vara tillsynsmyndighet även över Tullverkets behandling av personuppgifter i den brottsbekämpande verksamheten (se prop. 2004/05:164 s. 53 f.).

Datainspektionen har enligt 43 § personuppgiftslagen för sin tillsyn rätt att på begäran få tillgång till de personuppgifter som behandlas och upplysningar och dokumentation av behandlingen och säkerheten vid denna samt tillträde till sådana lokaler som har anknytning till behandlingen av personuppgifter. Om tillsynsmyndigheten inte, efter begäran enligt 43 § personuppgiftslagen, kan få tillräckligt underlag för att konstatera att behandlingen är laglig, får myndigheten enligt 44 § vid vite förbjuda den personuppgiftsansvarige att behandla personuppgifter på annat sätt än att lagra dem. Enligt 45 § ska myndigheten, om den konstaterar att uppgifter behandlas eller kan komma att behandlas på ett olagligt sätt, genom påpekanden eller liknande förfaranden försöka åstadkomma rättelse. Går det inte att få rättelse på annat sätt, eller är saken brådskande, får myndigheten på motsvarande

sätt förbjuda annan behandling än lagring. Tillsynsmyndigheten får också, enligt 47 §, ansöka hos länsrätten om att sådana uppgifter som har behandlats på olagligt sätt ska utplånas.

4.7.2 Säkerhets- och integritetsskyddsnämnden

Säkerhets- och integritetsskyddsnämnden ska enligt 1 § andra stycket lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet utöva tillsyn över Säkerhetspolisens behandling av uppgifter enligt polisdatalagen, särskilt vad avser behandling av känsliga personuppgifter. Tillsynen gäller utöver Datainspektionens tillsyn och ersätter alltså inte denna (se prop. 2006/07:133 s. 62).

Nämnden utövar enligt 2 § sin tillsyn genom inspektioner och andra undersökningar. De myndigheter som står under nämndens tillsyn ska lämna de uppgifter och det biträde som nämnden begär. Även domstolar och förvaltningsmyndigheter som inte står under nämndens tillsyn är skyldiga att lämna nämnden de uppgifter som den begär (4 §). Nämnden får uttala sig om konstaterade förhållanden och sin uppfattning om behovet av förändringar i verksamheten (2 § andra stycket).

Nämnden är enligt 3 § skyldig att på begäran av enskild kontrollera om han eller hon har varit föremål för personuppgiftsbehandling enligt 1 § och om behandlingen har skett i enlighet med lag eller annan författning. Nämnden ska underrätta den enskilde om att kontrollen har utförts. Däremot finns inget krav på att den enskilde ska få någon annan information om behandlingen.

4.8 Sekretess och tystnadsplikt

4.8.1 Allmänt om sekretesslagens reglering

För många av de personuppgifter som behandlas inom ramen för den brottsbekämpande verksamheten gäller sekretess. Sekretesslagen (1980:100) med tillhörande förordning innehåller bestämmelser om tystnadsplikt i det allmänna verksamheten och om förbud att lämna ut allmänna handlingar. Grundprincipen är att om det råder sekretess så gäller den även mellan myndigheter. Myndigheterna prövar frågan om utlämnande av uppgifter är tillåtet eller inte med stöd av sekretessregleringen. Sekretesslagen reglerar enbart offentlig verksamhet. För annan verksamhet finns i begränsad utsträckning regler om tystnadsplikt.

Det som är av störst intresse i detta sammanhang är sekretessen till skydd för den brottsbekämpande verksamheten och för enskilda vilkas uppgifter registreras i sådan verksamhet samt sekretessen för vissa register som används av de myndigheter som berörs av rambeslutet. Vidare har reglerna om utlämnande av sekretessbelagda uppgifter stor betydelse med tanke på rambeslutets tillämpningsområde.

4.8.2 Sekretess i brottsbekämpande verksamhet

Sekretess till skydd för brottsbekämpningen

I 5 kap. 1 § sekretesslagen finns regler till skydd för det allmänna brottsförebyggande och brottsbeivrande verksamheten. Sekretessen gäller bl.a. för anmälan om brott och i förundersökningar. Den gäller också i polisens, åklagarnas, Tullverkets, Skatteverkets och Kustbevakningens verksamhet i övrigt för att förebygga, uppdaga, utreda eller beivra brott. Sekretessen gäller om det kan antas att syftet med beslutade eller förutsedda åtgärder motverkas eller att den framtida verksamheten skadas om uppgiften röjs.

För Säkerhetspolisens verksamhet och för underrättelseverksamhet, oavsett vid vilken myndighet den bedrivs, gäller sekretess om det inte står klart att uppgiften kan röjas utan att syftet med beslutade eller förutsedda åtgärder motverkas eller att den framtida verksamheten skadas.

I de fall där en myndighet får uppgifter med sekretess enligt denna paragraf från en brottsbekämpande myndighet gäller sekretessen också hos mottagaren.

Sekretessen till skydd för brottsbekämpande verksamhet gäller enbart svensk sådan verksamhet. Därför har en särskild bestämmelse, som skyddar utländsk brottsbekämpande verksamhet, införts i 5 kap. 7 § sekretesslagen. Sekretess gäller i verksamhet som avser rättsligt samarbete på begäran av annan stat eller mellanfolklig domstol för uppgift som hänför sig till antingen utredning enligt bestämmelserna om förundersökning i brottmål eller angelägenhet som angår tvångsmedel, om det kan antas att det varit en förutsättning för den ansökandes begäran att uppgiften inte skulle röjas.

Motsvarande sekretess gäller hos polismyndighet eller åklagarmyndighet samt hos Rikspolisstyrelsen, Tullverket och Kustbevakningen för uppgift som avser framställningar enligt 3 § 1 och 6 lagen om Schengens informationssystem om viss åtgärd. Utan hinder av sekretessen får dock uppgifter lämnas ut enligt bestämmelser i den lagen eller i polisdatalagen.

Sekretess till skydd för enskild

I 9 kap. 17 § sekretesslagen regleras skyddet för enskildas personliga och ekonomiska förhållanden i brottsbekämpande verksamhet. Sekretess gäller bl.a. i utredning enligt reglerna om förundersökning i brottmål och i angelägenhet som rör användning av tvångsmedel. Sekretess gäller dessutom i polisens, åklagarnas, Tullverkets, Skatteverkets och Kustbevakningens verksamhet i övrigt för att förebygga, uppdaga, utreda eller beivra brott. Sekretessen gäller, om det inte står klart att uppgiften kan röjas utan

att den enskilde eller någon närstående till den enskilde lider skada eller men. Sekretess enligt denna bestämmelse överförs normalt inte till andra myndigheter, men de brottsbekämpande myndigheterna har i allt väsentligt samma sekretessreglering till skydd för enskilda.

Enligt 9 kap. 18 § sekretesslagen gäller sekretessen inte beslut i en åtalsfråga eller beslut om att en förundersökning inte ska inledas eller läggas ned. Den gäller inte heller i ärenden om ordningsbot eller strafföreläggande. Sekretessen enligt 17 § upphör i allmänhet att gälla om uppgiften lämnas till domstol med anledning av åtal. Däremot kan sekretessen föras över i andra fall (se avsnitt 4.8.4).

4.8.3 Sekretess för vissa register

Många register som innehåller ett stort antal personuppgifter som uppfattas som känsliga omgärdas av sekretess. Sekretessreglerna utgör i dessa fall ett skydd för den registrerade mot att uppgifter ur registren kommer i orätta händer. I de särskilda registerlagarna finns det dessutom i vissa fall regler om utlämnande av uppgifter som gäller i stället för den allmänna regleringen i sekretesslagen. I de fallen är skyddet extra starkt.

Enligt 7 kap. 17 § sekretesslagen gäller sekretess i verksamhet som avser förande av eller uttag ur register som förs enligt lagen (1998:620) om *belastningsregister*. Sekretessen är absolut, vilket innebär att någon skadeprövning inte behöver göras. Det är tillräckligt att konstatera om sekretessregeln är tillämplig. Utlämnande kan endast ske med stöd av regler i lagen om belastningsregister eller säkerhetsskyddslagen (1996:627) eller förordningar som har stöd i dessa lagar.

Sekretessen för *vissa andra polisregister* regleras i 7 kap. 18 § sekretesslagen. Enligt den paragrafen gäller sekretess bl.a. i verksamhet som avser förande av register eller uttag ur register

- för uppgift som har tillförts *strafförelägganderegister* (se avsnitten 4.4.9 och 4.5.4) eller *ordningsbotsregistret* (se avsnitt 4.4.8), och
- för annan uppgift hos Rikspolisstyrelsen som angår brott eller den som har misstänkts, åtalats eller dömts för brott, om uppgiften har lämnats dit för databehandling inom rättsväsendets informationssystem i andra register än de två nämnda.

Sekretessen för strafföreläggande- och ordningsbotsregistren gäller dock inte själva ärendet.

Även sekretessen för register enligt 7 kap. 18 § sekretesslagen är absolut, men i motsats till vad som gäller för uppgifter ur belastningsregistret kan uppgifter lämnas ut efter en sekretessprövning.

Sekretessen i 7 kap. 18 § sekretesslagen omfattar inte de register vars sekretess regleras i 9 kap. 17 § första stycket punkterna 6 och 7. Enligt den sistnämnda sekretessbestämmelsen gäller sekretess för uppgift om enskilds personliga eller ekonomiska förhållanden i register som förs av Rikspolisstyrelsen enligt polisdatalagen (1998:622) eller som annars behandlas där med stöd av samma lag (punkten 6) samt i register som förs enligt lagen (1998:621) om misstankeregister (punkten 7). Sekretessen gäller i dessa fall om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående lider skada eller men.

I samma paragraf regleras också sekretessen för

- *register som förs i Skatteverkets brottsbekämpande verksamhet* (punkten 8),
- *register som förs i Tullverkets brottsbekämpande verksamhet* (punkten 10),
- och
- *åklagarväsendets ärenderegister över brottmål* (punkten 9) med undantag för diarieuppgifter. Sekretessen för dessa register gäller under samma förutsättningar som för nyssnämnda polisregister.

Sekretess gäller också enligt 9 kap. 17 § första stycket punkten 4 i åklagarmyndighets, polismyndighets, Skatteverkets, Statens kriminaltekniska laboratoriums, Tullverkets eller Kustbevakningens verksamhet i övrigt för att förebygga, uppdaga, utreda eller beivra brott. Denna bestämmelse reglerar bl.a. sekretessen för sådana lokala polisregister som inte omfattas av sekretessen i 7 kap. 18 § eller 9 kap. 17 § första stycket punkterna 6 eller 7.

Enligt 9 kap. 17 § sjätte stycket punkten 3 sekretesslagen får, utan hinder av sekretess, en uppgift lämnas ut enligt vad som föreskrivs i lagen om misstankeregister, polisdatalagen, lagen om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar och lagen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet samt i förordningar som har stöd i dessa lagar. Syftet med bestämmelsen är bl.a. att myndigheterna inte ska behöva förlita sig på en sekretessprövning i de fall där det i författning anges att uppgifter får lämnas ut.

Enligt 9 kap. 31 § sekretesslagen gäller sekretess i verksamhet som avser förande eller uttag ur register som förs enligt lagen om passagerarregister (se avsnitt 4.4.7 om detta register) för uppgift om enskilds namn och födelsedatum samt nummer på resehandling. Sekretessen beträffande sådana uppgifter är absolut. Sekretess gäller också för uppgifter om enskilds ekonomiska förhållanden, om det kan antas att den enskilde lider skada om uppgiften röjs.

I 5 kap. 5 § sekretesslagen regleras sekretessen för *vapenregister* (se avsnitt 4.4.11 om dessa register). Sekretessen gäller bl.a. för förande av eller uttag ur vapenregister för uppgift som har tillförts registret, om det inte står klart att uppgiften kan röjas utan fara för att vapen eller ammunition kommer till brottslig användning. Sekretessen omfattar inte namn och adress på den som har tillstånd att driva handel med vapen och inte heller uppgift om vilka typer av vapen tillståndet omfattar.

4.8.4 Sekretess vid handläggning i domstol

Handlingar som ges in till domstol i brottmål är oftast inte sekretessbelagda. I de fall där en domstol i sin rättsskipande eller rättsvårdande verksamhet tar emot sekretessbelagda handlingar från en domstol eller annan myndighet gäller emellertid, enligt 12 kap. 1 § sekretesslagen, sekretessen även vid domstolen. Sekretess enligt 9 kap. 17 § första stycket 1, dvs. sekretess i utredning enligt bestämmelserna om förundersökning i brottmål, gäller enligt 12 kap. 2 § hos domstol endast om det kan antas att den enskilde eller någon närstående lider skada eller men om uppgiften röjs. Motsvarande gäller för sekretess i angelägenhet som avser användning av tvångsmedel (9 kap. 17 § första stycket 2). Sekretess för uppgift om vem som är misstänkt gäller dock bara vid fara för att den misstänkte eller någon närstående utsätts för våld eller annat allvarligt men om uppgiften röjs.

Huvudprincipen är att förhandlingar inför domstol är offentliga. Sekretessen för en uppgift upphör normalt att gälla hos domstolen om uppgiften förebringas vid en offentlig förhandling. Om uppgiften förebringas inför stängda dörrar fortsätter dock som regel sekretessen att gälla (12 kap. 3 §).

Sekretessen för en uppgift upphör också att gälla om uppgiften tas in i en dom eller ett beslut (12 kap. 4 §).

4.8.5 Sekretess för verkställighet av straffrättsliga påföljder

Enligt 7 kap. 21 § sekretesslagen gäller sekretess inom kriminalvården för uppgift om enskilds personliga förhållanden, om det kan antas att den enskilde eller någon närstående lider men eller att fara uppkommer för att någon utsätts för våld eller annat allvarligt men om uppgiften röjs. Sekretessen gäller dock inte för beslut i ärenden.

Enligt samma bestämmelse gäller sekretess hos regeringen i ärende om överförande av verkställighet av brottmålsdom för uppgift om enskilds personliga förhållanden, om det kan antas

att den enskilde eller någon närstående lider men eller att fara uppkommer för att någon utsätts för våld eller annat allvarligt men om uppgiften röjs. Sekretessen gäller dock inte regeringens beslut i ärenden.

Vidare gäller enligt 5 kap. 4 § sekretesslagen sekretess inom polisväsendet och Kriminalvården för uppgift om åtgärd som har till syfte att hindra rymning eller fritagning, om det kan antas att syftet med åtgärden motverkas om uppgiften röjs.

4.8.6 Sekretess för personuppgifter

I sammanhanget bör också nämnas att sekretess enligt 7 kap. 16 § sekretesslagen gäller för personuppgift, om det kan antas att ett utlämnande skulle medföra att uppgiften behandlas i strid med personuppgiftslagen. I fråga om behandling av personuppgifter för vilken datalagen (1973:289) alltjämt är tillämplig gäller fortfarande 7 kap. 16 § samt 9 kap. 6 och 7 §§ och 14 kap. 3 § sekretesslagen i deras äldre lydelse. Som framgått tidigare för polisen fortfarande många register med stöd av datalagen.

4.8.7 Utlämnande av sekretessbelagda uppgifter

Allmänt om sekretessbrytande regler

Enligt 1 kap. 3 § första stycket sekretesslagen får en sekretessbelagd uppgift hos en myndighet inte röjas för en annan myndighet utom i de fall som anges i sekretesslagen eller i lag eller förordning till vilken sekretesslagen hänvisar. Likaså gäller enligt andra stycket sekretess inom en myndighet mellan skilda verksamhetsgrenar.

De flesta sekretessbestämmelser förutsätter att sekretessbelagda uppgifter kan lämnas ut efter en bedömning i det enskilda fallet. Sekretessbestämmelser innehåller normalt ett skaderekvisit som kan vara rakt eller omvänt. Vid rakt skaderekvisit är pre-

sumtion för offentlighet medan presumptionen än den motsatta vid omvänt skaderekvisit. Vid absolut sekretess finns, som nyss nämnts, inget sådant skaderekvisit.

Generella sekretessbrytande regler finns framför allt i 14 kap. sekretesslagen, men även 1 kap. innehåller vissa sådana bestämmelser.

Sekretess hindrar enligt 1 kap. 5 § sekretesslagen inte att en uppgift lämnas ut, om det är nödvändigt för att den utlämnande myndigheten ska kunna fullgöra sina uppgifter. Inom den brottsbekämpande verksamheten måste t.ex. ofta sekretessbelagda uppgifter röjas i samband med förundersökning. Däremot får uppgifter inte lämnas ut med stöd av bestämmelsen om dessa skulle behövas i den mottagande myndighetens verksamhet.

I 14 kap. 1 § föreskrivs bl.a. att sekretess inte hindrar utlämnande till en annan myndighet om uppgiftsskyldighet följer av lag eller förordning. Uppgifter kan vidare, med vissa undantag, lämnas ut enligt 14 kap. 2 § när uppgifterna behövs i bl.a. förundersökningar. Enligt 14 kap. 3 §, den s.k. generalklausulen, gäller som huvudregel att uppgifter får lämnas ut till en annan myndighet, om det är uppenbart att intresset av att uppgiften lämnas har företräde framför det intresse som sekretessen ska skydda.

Enligt 15 kap. 5 § sekretesslagen ska en myndighet på begäran av en annan myndighet lämna uppgifter som den förfogar över, i den mån hinder inte möter på grund av sekretess eller av hänsyn till arbetets behöriga gång. Denna regel kan ses som en precisering av den allmänna skyldigheten att samverka och att lämna andra myndigheter hjälp inom ramen för den egna verksamheten.

I förhållandet mellan myndigheter är således huvudregeln att information både får och i viss utsträckning också ska utbytas, samtidigt som sekretesslagens regler begränsar de faktiska möjligheterna till informationsutbyte.

Dessa bestämmelser gäller dock enbart mellan svenska myndigheter.

Utlämnande till utländsk myndighet eller organisation

Utgångspunkten i sekretesslagen är att en uppgift, för vilken sekretess gäller, inte får röjas för en utländsk myndighet eller mellanfolklig organisation. I 1 kap. 3 § tredje stycket sekretesslagen finns dock bestämmelser som innebär att en sekretesskyddad uppgift får röjas för en utländsk myndighet eller mellanfolklig organisation i två situationer. Den ena är när utlämnandet sker i enlighet med särskild föreskrift i lag eller förordning. En uttrycklig bestämmelse om att uppgifter får lämnas till en utländsk myndighet eller organisation bryter alltså sekretess. Den andra är när uppgiften i motsvarande fall skulle få lämnas ut till en svensk myndighet och det enligt den utlämnande myndigheten står klart att det är förenligt med svenska intressen att uppgiften lämnas. Den sistnämnda bestämmelsen är, som framgår av lydelsen, avsedd att tillämpas restriktivt.

Särskilda regler om utlämnande till utländsk brottsbekämpande myndighet eller mellanfolklig organisation med brottsbekämpande uppgifter finns bl.a. i 7 § polisdatalagen och 17–18 §§ polisdataförordningen, 11 och 12 §§ lagen om belastningsregister, 9 och 10 §§ lagen om misstankeregister, 2 kap. 6 § lagen om internationellt tullsamarbete, 2 kap. 6 § lagen om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar och 18 § förordningen om behandling av personuppgifter inom åklagarväsendet.

Den nyss nämnda bestämmelsen i 1 kap. 5 § sekretesslagen har också viss betydelse i sammanhanget. I den brottsbekämpande verksamheten är det nämligen i ganska stor utsträckning nödvändigt att lämna sekretessbelagda uppgifter för att över huvud taget genomföra en brottsutredning. Ett typiskt exempel har ansetts vara att svenska myndigheter i samband med en begäran om rättslig hjälp i en förundersökning lämnar uppgifter som omfattas av sekretess enligt 5 kap. 1 § och 9 kap. 17 § sekretesslagen till en utländsk polis- eller åklagarmyndighet i syfte att få ett visst förhör genomfört. Om det är nödvändigt för en myndighet att lämna ut sekretessbelagda uppgifter för att myndigheten ska

kunna fullgöra sin egen verksamhet står det i regel klart att det är förenligt med svenska intressen att lämna uppgifterna.

4.8.8 Bestämmelser om tystnadsplikt i registerförfattningar

Några registerförfattningar innehåller bestämmelser om tystnadsplikt för den som får del av uppgifter ur registren. Sådana bestämmelser finns i 19 § lagen om belastningsregister och 14 § lagen om misstankeregister.

Bestämmelserna är utformade på samma sätt och innebär att den som med stöd av lagen har fått del av uppgifter om annans personliga förhållanden inte obehörigen får röja dessa uppgifter. Den som bryter mot en sådan tystnadsplikt kan straffas enligt 20 kap. 3 § brottsbalken.

Regleringen ska ses mot bakgrund av att den som bedriver viss verksamhet, bl.a. den som beslutar om anställning av personer inom psykiatrisk vård, vård av utvecklingsstörda eller vård av barn och ungdom, kan ha rätt att få utdrag ur registren i fråga även om verksamheten bedrivs i privat regi. Registerkontroll är numera obligatorisk inom vissa sektorer av det allmänna, se exempelvis lagen (2000:783) om registerkontroll av personal inom förskoleverksamhet, skola och barnomsorg.

I det allmännas verksamhet tillämpas, som tidigare nämnts, i stället sekretesslagen.

4.9 Regler om informationssäkerhet

I 9 § säkerhetsskyddslagen (1996:627) finns vissa regler om informationssäkerhet. Dessa syftar till skydda sekretessbelagda handlingar som rör rikets säkerhet mot att dessa röjs, ändras eller förstörs (6 och 7 §§). I 12 § säkerhetsskyddsförordningen finns ytterligare föreskrifter med inriktning på skyddet för register och system för automatisk databehandling som innehåller sekretessbelagda uppgifter av nyss nämnt slag. Vidare före-

skrivs att myndigheter och andra som omfattas av reglerna i förordningen ska förvissa sig om att mottagaren har fullgod informationssäkerhet innan de sänder hemliga uppgifter i ett datanät utanför deras kontroll.

Regelverket om arkivering räknas också som bestämmelser om informationssäkerhet (prop. 1997/98:44 s. 92). Som exempel kan nämnas reglerna i 3, 5 och 6 §§ arkivlagen (1990:782) om hur arkivhandlingar och arkiv ska hanteras.

Vidare bör nämnas att regeln i 5 kap. 2 § sekretesslagen om sekretess för uppgift som lämnar eller kan bidra till upplysning om säkerhets- eller bevakningsåtgärd med avseende på byggnader eller andra anläggningar, lokaler eller inventarier har ansetts gälla för uppgifter om en tingsrätts datorer och tillhörande utrustning (RÅ 2004:97).

5 Internationellt samarbete

5.1 Allmänna utgångspunkter

Rambeslutets tillämpningsområde omfattar endast sådana uppgifter som överförs eller görs tillgängliga mellan stater inom Europeiska unionen eller mellan en medlemsstat och ett tredje land eller ett internationella organ som sysslar med brottsbekämpning. Till de sistnämnda hör framför allt Europol och Interpol. Frågan om informationsutbyte i det internationella samarbetet har därför särskild betydelse. I detta avsnitt redovisas dels lagstiftningen om internationellt samarbete inom de verksamhetsområden som berörs av rambeslutet, dels samarbetet med några internationella organ.

5.2 Regler om användningsbegränsningar

Från slutet av 1980-talet föreslogs allt oftare vid förhandlingar om internationella överenskommelser om rättsligt samarbete och informationsutbyte bestämmelser om begränsningar i fråga om hur överlämnad information får användas. Det väckte så småningom frågan om hur man skulle hantera den typen av bestämmelser i svensk rätt. Eftersom Sverige följer den dualistiska rättstraditionen krävs det svensk lagstiftning för att införliva bindande förpliktelser i internationella överenskommelser med svensk rätt.

För att undvika en konflikt mellan å ena sidan ett folkrättsligt bindande åtagande om att hantera viss information i enlighet

med de villkor som ställts upp av den stat som överlämnat informationen och å andra sidan den svenska lagstiftningen ansågs det så småningom vara nödvändigt med en lagreglering.

Mot bakgrund av att det på brottmålsområdet finns en rad tvingande regler, framför allt polisens och åklagares skyldighet att inleda förundersökning när det finns objektiv grund för det och åklagares åtalsplikt, infördes en generell lagstiftning som skulle täcka begränsningar i fråga om användning av viss typ av information, s.k. användningsbegränsningar. Om det i en överenskommelse som Sverige ingått med främmande stat fanns ett villkor om att upplysningar eller bevismaterial som erhållits från en främmande stat endast fick användas på visst sätt eller för visst ändamål eller begränsades på annat sätt, skulle villkoret följas oavsett vad som annars var föreskrivet i lag eller annan författning. Bestämmelsen togs in i lagen (1991:435) med särskilda bestämmelser om internationellt samarbete på brottmålsområdet.

Lagen upphävdes när lagen (2000:562) om internationell rättslig hjälp i brottmål (se avsnitt 5.4.1) infördes. Numera finns det således ingen generell lagstiftning på området utan motsvarande bestämmelser finns i flera olika lagar. En beskrivning av utvecklingen därefter finns i prop. 2004/05:144 s. 152 ff.

Det förhållandet att en regel om användningsbegränsning finns i en lag som primärt gäller för ett visst verksamhetsområde får inte tolkas så att den bara ska tillämpas i den verksamheten. Tvärtom gäller en användningsbegränsning för alla svenska myndigheter. JO har i ett ärende som berörde flera myndigheter utvecklat detta närmare. JO framhöll också att sådana uppgifter som erhållits för brottsbekämpning och som eventuellt inflyter i en dom inte heller får användas fritt om de omfattas av en användningsbegränsning (JO 2007/08 s. 57).

Det bör anmärkas att de flesta internationella överenskommelser som innehåller bestämmelser som begränsar rätten att använda information eller bevismaterial erbjuder en möjlighet att begära den översändande statens samtycke till annan användning.

5.3 Samarbete i den brottsbekämpande verksamheten

5.3.1 Lagstiftningen om polissamarbete

Lagen om internationellt polisiärt samarbete

I lagen (2000:343) om internationellt polisiärt samarbete finns bestämmelser om samarbete mellan svenska brottsbekämpande myndigheter och motsvarande myndigheter i andra medlemsstater i Europeiska unionen samt Norge och Island. Lagen reglerar bl.a. Schengensamarbetet men även annat polissamarbete som är konventionsbundet. I lagen anges vilka svenska tjänstemän som är behöriga att delta i samarbetet. Dessa är svenska polismän, tulltjänstemän och kustbevakningstjänstemän, när de enligt lag eller annan författning har polisiära befogenheter.

Den viktigaste delen av informationsutbytet inom Schengensamarbetet regleras i lagen om Schengens informationssystem (se avsnitt 4.4.6). Den nu aktuella lagen reglerar annat samarbete och informationsutbyte som är mera inriktat på enskilda fall.

I lagen finns en bestämmelse (3 §) om hur uppgifter som har erhållits från andra stater får användas. Bestämmelsen motsvarar i huvudsak 1 § i den upphävda lagen med särskilda bestämmelser om internationellt samarbetet på brottmålsområdet. Har en svensk myndighet fått upplysningar eller bevismaterial från en annan stat för att användas i underrättelseverksamhet om brott eller vid utredning av brott, och gäller på grund av överenskommelse med den andra staten villkor som begränsar möjligheten att utnyttja materialet, ska svenska myndigheter följa villkoren oavsett vad som annars är föreskrivet i lag eller annan författning. Vad som nu har sagts gäller även för överenskommelser med mellanfolkliga organisationer. Sistnämnda tillägg gjordes när EES-avtalet infördes.

Lagen om vissa former av internationellt samarbete i brottsutredningar

Lagen (2003:1174) om vissa former av internationellt samarbete i brottsutredningar genomför rådets rambeslut 2002/465/RIF av den 13 juni 2002 om gemensamma utredningsgrupper och konventionen av den 29 maj 2000 om ömsesidig rättslig hjälp i brottmål mellan Europeiska unionens medlemsstater (1 §). Vissa av lagens bestämmelser tillämpas också på det avtal som träffats mellan Europeiska unionen och Island och Norge om tillämpning av vissa bestämmelser i nämnda konvention.

Syftet med rambeslutet är att förbättra det polisiära och det straffrättsliga samarbetet mellan Europeiska unionens medlemsstater i kampen mot den gränsöverskridande brottsligheten. Behöriga myndigheter i två eller flera medlemsstater får genom en överenskommelse inrätta en gemensam utredningsgrupp för brottsutredningar i en eller flera av de medlemsstater som inrättar gruppen. När det finns en sådan överenskommelse, mellan en eller flera myndigheter i Sverige och motsvarande myndigheter i en eller flera andra medlemsstater, tillämpas lagen. De utredningsgrupper som inrättas med stöd av någon annan internationell överenskommelse omfattas inte av lagen. Bestämmelser om gemensamma utredningsgrupper finns även konventionen upprättad på grundval av artikel K 3 i fördraget om Europeiska unionen om ömsesidigt bistånd och samarbetet mellan tullförvaltningar (tullsamarbetskonventionen), som genomförts genom lagen om internationellt tullsamarbete (se nedan).

En gemensam utredningsgrupp får endast inrättas för ett särskilt syfte och för begränsad tid (2 §). Om förundersökning har inletts i Sverige, får beslut om inrättande av en utredningsgrupp fattas av den åklagare eller den myndighet som leder förundersökningen. Om svensk förundersökning varken pågår eller inleds kan bl.a. riksåklagaren, Rikspolisstyrelsen, Kustbevakningen eller Tullverket besluta om att inrätta en gemensam utredningsgrupp (3 §).

Om en åklagare beslutar om att inrätta en utredningsgrupp med svenskt deltagande kan även polismän, tulltjänstemän eller tjänstemän från Kustbevakningen delta i denna.

Det ska framgå av överenskommelsen vilka tjänstemän som ingår i den gemensamma utredningsgruppen och under vilken tid gruppen ska vara verksam.

Om det för den gemensamma utredningsgruppens arbete krävs att en utredningsåtgärd vidtas i Sverige, och åtgärden i fråga inte kan utföras inom ramen för en pågående svensk förundersökning, kan en svensk tjänsteman som deltar i utredningsgruppen ansöka om den utredningsåtgärd som behövs för den gemensamma gruppens arbete i Sverige. I fråga om en sådan ansökan tillämpas lagen om internationell rättslig hjälp i brottmål på motsvarande sätt som om ansökan hade gjorts av en utländsk myndighet (4 §), se nästa avsnitt.

Vidare innehåller lagen bestämmelser om användningsbegränsningar. Har en svensk myndighet fått uppgifter genom en gemensam utredningsgrupp som inrättats med stöd av lagen och gäller på grund av en överenskommelse som anges i 1 § villkor som begränsar möjligheten att använda uppgifterna, ska en svensk myndighet enligt 5 § följa villkoren oavsett vad som annars är föreskrivet i lag eller författning. Enligt 6 § får överlämnandet av uppgifter eller bevismaterial från en svensk myndighet till en sådan utredningsgrupp förenas med villkor som är nödvändiga av hänsyn till enskilds rätt eller som är nödvändiga från allmän synpunkt. Villkor som strider mot en överenskommelse enligt 1 § får dock inte ställas upp.

Den svenska myndighet som har överlämnat material med ett sådant villkor får enligt 7 § på begäran av en myndighet i en annan stat medge undantag från villkor enligt 6 §. Detsamma gäller för villkor som följer direkt av en överenskommelse som träffats med stöd av 1 §.

Lagen innehåller också vissa bestämmelser om s.k. kontrollerade leveranser (10–14 §§). Med detta avses att en viss förbjuden vara, oftast narkotika, tillåts passera gränsen utan att myndigheterna ingriper, i syfte att man ska kunna spåra upp de personer

som ligger bakom brottet. Den delen av lagen är generell, dvs. den gäller för överenskommelser även med andra stater än sådana som kan ingå i en gemensam utredningsgrupp.

Vidare finns bestämmelser om brottsutredningar med användning av skyddsidentitet (15–17 §§). Även den regleringen är generell.

Både vid kontrollerade leveranser och vid brottsutredningar med användning av skyddsidentitet ska reglerna om användningsbegränsning i 5–7 §§ tillämpas (13 respektive 16 §).

Lagen om Schengens informationssystem

I avsnitt 4.4.6 finns en redogörelse för lagen om Schengens informationssystem (SIS). Även den lagen innehåller en regel om användningsbegränsning (10 §). Enligt den bestämmelsen får en svensk myndighet inte utnyttja en uppgift i registret för något annat syfte än det som den registrerande staten har angett vid registreringen. De ändamål för registrering som anges i 2 och 3 §§ samma lag är framställningar om

- omhändertagande av en person som efterlysts för överlämnande eller utlämning,
- att en person ska nekas tillträde till eller uppehållstillstånd i Schengenstaterna,
- uppgift om uppehållsorten för en person som är anmäld försvunnen,
- tillfälligt omhändertagande av en person med hänsyn till dennes eller annans säkerhet,
- uppgift om var den uppehåller sig som ska inställa sig vid domstol i brottmålsförhandling, som ska dömas eller inställa sig för verkställighet av frihetsberövande,
- dold övervakning eller särskilda kontrollåtgärder, och
- åtgärder beträffande fordon eller föremål som har efterlysts för att tas i beslag eller användas som bevismaterial i brottmålsrättegång.

Om den registrerande staten har lämnat sitt samtycke, får dock en svensk myndighet använda uppgiften för annat ändamål.

5.3.2 Lagen om internationellt tullsamarbete

Liksom det finns ett internationellt polissamarbete, samarbetar Tullverket med andra länders tullmyndigheter och andra behöriga myndigheter. Det internationella tullsamarbetet bygger, såvitt nu är av intresse, dels på bilaterala tullsamarbetsavtal, dels på internationella konventioner. De i detta sammanhang viktigaste internationella konventionerna är Världstullorganisationens (se avsnitt 5.6.5) konvention den 9 juni 1977 om ömsesidigt administrativt bistånd för att förhindra, utreda och beivra tullbrott (prop. 1982/83:35), dels Europeiska unionens tullsamarbetskonvention (prop. 1999/2000:122).

Samarbetet regleras i lagen (2000:1219) om internationellt tullsamarbete. Syftet är att förhindra, upptäcka, utreda och beivra överträdelser av tullbestämmelser. I lagen anges att Tullverket eller annan behörig svensk myndighet ska bistå utländsk myndighet och mellanfolklig organisation. Behöriga myndigheter är, förutom Tullverket, Rikspolisstyrelsen, polismyndigheter, Kustbevakningen och Statens jordbruksverk (1 kap. 5 §). Tullverket har ansvaret för samordningen av samarbetet.

Vid internationellt tullsamarbete kan de svenska myndigheterna agera endast inom ramen för sina befogenheter enligt nationell lagstiftning (1 kap. 3 §).

Samarbetet får inte innebära att en åtgärd vidtas som strider mot svensk författning eller svenska allmänna rättsprinciper. Samarbetet består bl.a. i att länderna självmant eller efter ansökan ska delge varandra uppgifter som behövs för tullsamarbetet. Svensk myndighet har också rätt att inleda utredning om överträdelse av tullbestämmelser i en annan stat. I en sådan utredning får utländsk tjänsteman närvara.

Bestämmelser om utbyte av uppgifter finns i 2 kap. 6–8 §§. När det är nödvändigt för att genomföra internationellt tullsamarbete

enligt lagen, eller på eget initiativ eller efter ansökan, får en svensk behörig myndighet lämna ut uppgifter till behörig utländsk myndighet eller mellanfolklig organisation. Detta gäller även om uppgiften är sekretessbelagd (2 kap. 6 §), men omfattar endast uppgifter som är tillgängliga för myndigheten inom dess verksamhetsområde. Uppgifter som lämnas ut enligt den paragrafen får förenas med villkor för användandet, om det krävs med hänsyn till enskilds rätt eller från allmän synpunkt (2 kap. 7 §).

Har en svensk myndighet översänt en uppgift till en utländsk myndighet enligt 2 kap. 6 §, är myndigheten skyldig att på begäran av den som uppgiften avser underrätta denne om vilken utländsk myndighet eller mellanfolklig organisation som uppgiften översänts till och för vilket ändamål. Detta gäller dock inte om det är uppenbart obehövt eller om det kan befaras att underrättelsen skulle försvåra den utländska myndighetens eller organisationens utredning eller beslut. Gäller sekretess enligt 5 kap. 1 § sekretesslagen för uppgiften behöver underrättelse inte heller lämnas (2 kap. 8 §).

Lagen innehåller också bestämmelser om användningsbegränsningar. I 4 kap. 2 § föreskrivs att om en svensk myndighet har tagit emot uppgifter eller bevisning från en annan stat enligt en internationell överenskommelse som innehåller villkor som begränsar möjligheten att använda uppgifterna, ska svenska myndigheter följa villkoren oavsett vad som annars är föreskrivet i lag eller annan författning. De överenskommelser som avses är sådana överenskommelser med en annan stat eller en mellanfolklig organisation som Sverige är bunden av och som har till syfte att upptäcka, utreda eller beivra överträdelser av tullbestämmelser (1 kap. 1 §). Lagen är dock inte tillämplig på sådant samarbete som avses i lagen (1969:200) om uttagande av utländsk tull, annan skatt, avgift eller pålaga eller lagen (1959:590) om gränstullsamarbete med annan stat.

5.4 Lagstiftningen om internationellt rättsligt samarbete

5.4.1 Internationell rättslig hjälp i brottmål

I lagen (2000:562) om internationell rättslig hjälp i brottmål finns bestämmelser om skyldigheten att på utländsk myndighets begäran vidta åtgärder som bl.a. förhör under förundersökning, bevisupptagning, telefonförhör, kvarstad, husrannsakan och användning av hemliga tvångsmedel (1 kap. 2 §). I lagen finns motsvarande bestämmelser om hur Sverige kan begära rättslig hjälp utomlands (3 kap.). Det närmare förfarandet för sådana framställningar regleras i förordningen (2000:704) om internationell rättslig hjälp i brottmål.

Lagen om internationell rättslig hjälp är generell, dvs. den gäller i förhållande till alla stater även om dessa inte har tillträtt samma konventioner om rättslig hjälp i brottmål som Sverige. I lagens fjärde kapitel finns dock numera vissa regler som bara gäller i förhållande till medlemsstater i Europeiska unionen samt Norge och Island.

En utländsk stats begäran om rättslig hjälp i Sverige handläggs av åklagare och domstol, under förutsättning att åtgärden kan vidtas enligt svensk lag under en förundersökning eller rättegång. I vissa fall får rättslig hjälp beviljas, även om den misstänkta gärningen inte utgör brott enligt svensk lagstiftning (2 kap. 2 §).

I 2 kap. finns allmänna bestämmelser om förfarandet vid en ansökan om rättslig hjälp i Sverige. Framställningar om rättslig hjälp ska handläggas skyndsamt. I princip används samma förfarande som vid motsvarande svensk åtgärd under förundersökning eller rättegång (2 kap. 10 §). Åklagaren anses vid verkställigheten av en begäran om rättslig hjälp kunna begära biträde av en polismyndighet, Tullverket eller Kustbevakningen i samma utsträckning som för en motsvarande svensk förundersökningsåtgärd.

I 4 kap. regleras vissa former av rättslig hjälp närmare, framför allt användning av olika typer av tvångsmedel.

Om en svensk myndighet i ett ärende om rättslig hjälp har fått uppgifter eller bevisning från en annan stat för att användas vid utredning av brott eller i ett rättsligt förfarande med anledning av brott, och gäller på grund av en internationell överenskommelse som är bindande för Sverige villkor som begränsar möjligheterna att använda uppgifterna eller bevisningen, ska, enligt 5 kap. 1 §, villkoret följas oavsett vad som annars är föreskrivet i lag eller annan författning.

Detsamma gäller beträffande villkor som en stat har ställt upp när den på eget initiativ lämnar sådana uppgifter.

Enligt 5 kap. 2 § får rättslig hjälp som lämnas av en svensk myndighet i enskilda fall förenas med villkor som är påkallade med hänsyn till enskilds rätt eller som är nödvändiga ur allmän synpunkt. Detsamma gäller för uppgifter som lämnas i form av rättslig hjälp utan samband med ett ärende. Villkor som strider mot en internationell överenskommelse som är bindande för Sverige får dock aldrig ställas.

Den åklagare eller den domstol som har ställt ett villkor enligt 5 kap. 2 § får enligt 5 kap. 3 § på begäran av en myndighet i den mottagande staten medge undantag från villkoret.

5.4.2 Överlämnande från Sverige enligt en europeisk arresteringsorder

Inom Europeiska unionen tillämpas ett förenklat förfarande för utlämning med anledning av brott. Om en medlemsstat har meddelat ett rättsligt avgörande och begär att en annan stat ska gripa och överlämna en eftersökt person för lagföring eller verkställighet tillämpas lagen (2003:1156) om överlämnande från Sverige enligt en europeisk arresteringsorder. Lagen tillämpas också för överlämnande av svenska medborgare. Regleringen genomför rådets rambeslut 2002/584/RIF av den 13 juni 2002 om en europeisk arresteringsorder och överlämnande mellan medlemsstaterna.

I lagen anges att överlämnande ska ske antingen om överlämnandet avser lagföring (om gärningen utgör brott enligt svensk lagstiftning samt det för brottet är föreskrivet en frihetsberövande påföljd i ett år eller mer) eller om överlämnandet avser verkställighet (och den utdömda påföljden innebär ett frihetsberövande i minst fyra månader), se 2 kap. 2 §. I lagen anges också när överlämnande inte får ske (2 kap. 3–6 §§). Det gäller bl.a. om arresteringsordern är bristfällig, om den eftersökte ska överlämnas till tredje stat eller Internationella brottmålsdomstolen, om den dömde var under 15 år när gärningen begicks eller om överlämnandet skulle strida mot Europakonventionen.

En arresteringsorder kan översändas genom Schengens informationssystem eller annat system för eftersökning av personer som är misstänkta för brott. En arresteringsorder kan också skickas direkt till behörig åklagare i den region där man antar att den eftersökte befinner sig (4 kap. 1 §).

Allmän åklagare är ansvarig för handläggningen av ärenden enligt lagen. Åklagaren utreder om det finns grund för överlämnande och fattar beslut om anhållande av eller reseförbud eller anmälningsplikt för den efterlyste (4 kap. 3 §). Allmän domstol beslutar om överlämnande, men åklagaren får avslå en begäran.

I brådskande fall får en polisman, tulltjänsteman eller tjänsteman vid Kustbevakningen även utan ett anhållningsbeslut gripa den som är efterlyst i en arresteringsorder som översänts t.ex. genom Schengens informationssystem (4 kap. 5 § fjärde stycket lagen). Polisen, Tullverket och Kustbevakningen har direktåtkomst till SIS-registret, enligt 10 § förordningen (2000:836) om Schengens informationssystem.

När någon har gripits ska åklagaren genast inleda en utredning om det finns förutsättningar för överlämnande från Sverige. Utredningen ska göras enligt bestämmelserna om förundersökning i brottmål.

5.4.3 Erkännande och verkställighet av frysningsbeslut

Inom Europeiska unionen tillämpas också ett förenklat förfarande för verkställighet av beslut om frysning av egendom eller bevismaterial. Lagen (2005:500) om erkännande och verkställighet i Europeiska unionen av frysningsbeslut genomför rådets rambeslut 2003/577/RIF av den 22 juli 2003 om verkställighet i Europeiska unionen av beslut om frysning eller bevismaterial.

Med frysningsbeslut avses i lagen dels beslut om kvarstad enligt 26 kap. rättegångsbalken, som avser värdet av förverkad egendom, dels ett svenskt beslut om beslag enligt lagen, dels vissa motsvarande beslut som har meddelats av en rättslig myndighet i en annan medlemsstat. Handläggningen i Sverige sköts av åklagare enligt de närmare bestämmelser som anges i lagen samt i förordningen (2005:501) om erkännande och verkställighet inom Europeiska unionen av frysningsbeslut.

Verkställigheten i Sverige av ett utländskt frysningsbeslut sker enligt reglerna i 27 kap. 10–13 §§ rättegångsbalken om det är fråga om beslag och enligt reglerna om kvarstad i brottmål om frysningsbeslutet avser verkställighet av värdet av förverkad egendom (3 kap. 6 § lagen). Vid verkställigheten av beslag får husrannsakan, kroppsvisitation eller kroppsbesiktning göras enligt reglerna i 28 kap. rättegångsbalken (3 kap. 10 § lagen). Vid verkställighet av kvarstadsbeslut får egendom tas i förvar till dess att frysningsbeslutet har verkställts (3 kap. 11 § lagen).

Vid verkställighet av frysningsbeslut avseende beslag samt när egendom ska tas i förvar ska polismyndighet, Tullverket eller Kustbevakningen biträda åklagaren (3 kap. 12 § lagen).

Genom 3 kap. 13 § lagen utvidgas åklagares rätt att få tillgång till uppgifter ur belastningsregistret och misstankeregistret.

5.4.4 Rambeslut om en europeisk bevisinhämtningsorder

Den 14 november 2003 presenterade Europeiska unionens kommission ett förslag till rådets rambeslut om en europeisk bevisin-

hämtningsorder. Avsikten är att genom rambeslutet och andra instrument på sikt ersätta den traditionella rättsliga hjälpen med enklare förfaranden. Bevisinhämtningsordern är tänkt att utgöra steget efter ett frysningsbeslut.

Rambeslutet är inriktat på föremål, handlingar och uppgifter som erhållits genom processrättsliga åtgärder och som är direkt tillgängliga. Det innebär att bevismaterial som först har varit föremål för ett frysningsbeslut därefter kan bli föremål för en bevisinhämtningsorder. Rambeslutet bygger vidare på principen om ömsesidigt erkännande.

Rambeslutet omfattar inte förhör med misstänkta, tilltalade, vittnen eller offer, förutom i ett avseende, nämligen vittnesmål av personer som är närvarande vid verkställigheten av en bevisinhämtningsorder. Rambeslutet omfattar inte heller inhämtning av uppgifter i realtid eller bevisning i form av sådana föremål, handlingar eller uppgifter som kräver någon form av ytterligare utredning eller analys.

För en närmare beskrivning av rambeslutet hänvisas till departementspromemorian Sveriges antagande av rambeslutet om en europeisk bevisinhämtningsorder (Ds 2008:9). Promemorian är föremål för remissbehandling.

5.4.5 Rambeslut om utbyte av information ur kriminalregister

I Haagprogrammet uppmanades kommissionen bl.a. att framlägga förslag till ökat utbyte av uppgifter om domar i nationella register.

I januari 2006 lade kommissionen fram ett förslag till rambeslut om utbyte av information ur kriminalregister. Utkastet till rambeslut innebär en utveckling av artiklarna 13 och 22 i Europarådets konvention från 1959 om ömsesidig rättslig hjälp i brottmål. Arbetet ska ske i två faser. I första steget åtar sig medlemsstaterna att dels mer regelbundet informera varandra när en person döms för brott i en medlemsstat men denne är medbor-

gare i en annan medlemsstat, dels effektivisera informationsutbytet när uppgifter begärs i ett enskilt ärende. I den andra fasen av arbetet är målet att denna information ska kunna utbytas elektroniskt med hjälp av ett standardiserat format.

Medlemsstaterna ska så snart som möjligt informera den medlemsstat i vilken den dömda är medborgare om en dom i brottmål. Vidare ska det med domen följa information om hur länge en registrering kommer att finnas kvar i domslandets kriminalregister. Information om de ändringar eller den gallring av uppgifter som sker i kriminalregistret ska också översändas till den medlemsstat som fått information om domen.

När information ur kriminalregistret begärs i en medlemsstat finns det möjlighet att även begära information från en annan stats kriminalregister. Detta gäller även när en enskild person efterfrågar uppgifter om sig själv, under förutsättning att personen är eller har varit bosatt eller är medborgare i den andra staten.

En myndighets begäran om information ur kriminalregister ska besvaras omedelbart eller i vart fall inom tio arbetsdagar. Kommer förfrågan från en privatperson ska information lämnas inom 20 arbetsdagar.

Uppgifter som erhålls från en annan stat får användas endast för det ändamål för vilket uppgifterna begärdes. De får dock alltid användas för att avvärja omedelbara och allvarliga hot. Dessutom kan den andra staten medge användning för andra ändamål, men kan då ställa upp särskilda villkor.

Slutligen ska medlemsstaterna inom tre år efter antagandet av rambeslutet genomföra de tekniska åtgärder som krävs för att information ur kriminalregister ska kunna överföras elektroniskt.

En politisk överenskommelse har nåtts om innehållet i rambeslutet. Inom Regeringskansliet pågår arbetet med att ta fram underlag för genomförandet av rambeslutet.

5.5 Lagstiftning om samarbete i fråga om verkställighet av påföljder

5.5.1 Allmänt

Det internationella samarbetet om överförande av verkställighet av straffrättsliga påföljder mellan Sverige och andra stater sker ofta på avtalsrättslig grund. Det finns emellertid flera internationella överenskommelser om överförande av straffverkställighet som Sverige har ingått och som har genomförts i svensk lagstiftning. Dessa redovisas i korthet nedan. För en närmare redogörelse för lagstiftningen när det gäller verkställighet av frihetsberövande straff hänvisas till Ds 2008:1 Sveriges antagande av rambeslut om överförande av frihetsberövande påföljder inom Europeiska unionen, s. 21 ff. och för motsvarande redovisning när det gäller bötesstraff hänvisas till Ds 2007:18 Verkställighet inom Europeiska unionen av bötesstraff och beslut om förverkande, s. 86 ff.

5.5.2 Internationella verkställighetslagen

Enligt 1 § lagen (1972:260) om internationellt samarbete rörande verkställighet av brottmålsdom (internationella verkställighetslagen) får regeringen bestämma att domar avseende frihetsberövande, böter eller förverkande, som har dömts ut i andra stater, får verkställas i Sverige eller att svenska påföljder får verkställas i en annan stat, i den mån det följer av en överenskommelse som Sverige har ingått med en annan stat. De viktigaste överenskommelserna är 1970 års konvention om brottmålsdoms internationella rättsverkningar (brottmålsdomskonventionen), 1983 års konvention om överförande av dömda personer (överförandekonventionen) och 1990 års tillämpningskonvention till Schengenavtalet (Schengenkonventionen).

Även om det inte finns något bilateralt eller multilateralt avtal om överförande av verkställighet kan regeringen enligt 3 § lagen,

om det föreligger synnerliga skäl i ett enskilt fall, genom regeringsbeslut förordna att en frihetsberövande påföljd som har dömts ut i Sverige får verkställas i en annan stat eller att en sådan påföljd som har ådömts en svensk medborgare eller en utlänning med hemvist i Sverige får verkställas här. Vid verkställighet enligt brottmålsdomskonventionen och enligt överförandekonventionen krävs dubbel straffbarhet, dvs. gärningen ska utgöra brott enligt svensk lagstiftning.

Om ett straff verkställs i Sverige efter överförande hit sker verkställigheten enligt svenska regler. Straff som är strängare än vad som är möjligt att utdöma enligt svensk lag kan förekomma.

Lagen innehåller få regler av allmän karaktär. Flertalet bestämmelser reglerar de specifika förutsättningar och förfaranden som gäller enligt respektive konvention.

Överförandekonventionen syftar i första hand till att främja dömda personers återanpassning till samhället. Konventionen innebär inte någon skyldighet att överföra eller överta straffverkställighet. Ett överförande förutsätter alltid både domslandets och den verkställande statens samtycke. Den dömde själv måste också samtycka till överförandet.

Samtliga medlemsstater i Europeiska unionen har tillträtt överförandekonventionen. Flertalet överföranden inom Europa sker med stöd av den. Överförande inom Norden sker dock alltså normalt med stöd av den nordiska verkställighetslagen, som beskrivs närmare i ett följande avsnitt.

Enligt Schengenkonventionen kan överförande av verkställighet i princip ske enligt samma förutsättningar som gäller enligt överförandekonventionen, men utan den dömdes samtycke om denne har flytt för att undandra sig verkställighet av en dom i domslandet, eller om den dömde enligt domen ska utvisas eller annars inte får vistas i domslandet. Regleringen gäller i förhållande till de stater som ingår i Schengensamarbetet och är bundna av Schengenkonventionen i relevanta delar.

Överföranden enligt brottmålsdomstolskonventionen förekommer sällan eftersom förfarandet upplevs som komplicerat. Brottmålsdomskonventionen har samma syfte som överförande-

konventionen, men innebär en förpliktelse för en stat att överta verkställigheten om förutsättningarna för detta är uppfyllda. Förfarandet är mera detaljreglerat än förfarandet enligt överförandekonventionen, bl.a. på det sättet att det krävs ett domstolsbeslut i den stat som övertar verkställigheten.

5.5.3 Rambeslut om överförande av frihetsberövande påföljder inom Europeiska unionen

I januari 2005 tog Österrike, Finland och Sverige initiativ till ett rambeslut om överförande av dömda mellan Europeiska unionens medlemsstater. Vid rådets för rättsliga och inrikes frågor möte den 15 februari 2007 nåddes en principöverenskommelse om innehållet i rambeslutet.

Rambeslutet bygger vidare på den av europeiska rådet i Tammerfors år 1999 antagna principen om att ömsesidigt erkännande ska vara hörnstenen i det rättsliga samarbetet mellan Europeiska unionens medlemsstater. Innebörden i rambeslutet är att medlemsstaterna ska erkänna och verkställa varandras avgöranden utan någon vidare prövning. I rambeslutet är prövningen av om en annan stats avgörande ska erkännas och verkställas begränsad till några få omständigheter (vägransgrunder). Om en sådan omständighet föreligger, får erkännande och verkställighet vägras. I annat fall ska den tillfrågade staten överta verkställigheten av påföljden.

Regeringen har nyligen lagt fram en proposition om godkännande av rambeslutet (prop. 2007/08:84).

5.5.4 Nordiska verkställighetslagen

För de nordiska länderna finns en enhetlig och i princip likalydande lagstiftning om överförande av verkställighet av straff. Lagen (1963:193) om samarbete med Danmark, Finland, Island

och Norge angående verkställighet av straff m.m. (nordiska verkställighetslagen) reglerar förfarandet.

De nordiska lagarna möjliggör verkställighet av böter, förverkande, frihetsstraff och övervakning av villkorligt dömda och villkorligt frigivna. Verkställighet av överlämnande till särskild vård regleras inte i lagen, men då kan i stället överförandekonventionen eller internationella verkställighetslagen tillämpas; se 13 § andra stycket förordningen (1977:178) med vissa bestämmelser om internationellt samarbete rörande verkställighet av brottmålsdom.

Fängelsestraff som har dömts ut i ett annat nordiskt land får enligt den nordiska verkställighetslagen verkställas i Sverige, om den dömda är svensk medborgare eller har hemvist här eller, om personen befinner sig i Sverige, det med hänsyn till omständigheterna är lämpligast. Under motsvarande förutsättningar får ett svenskt fängelsestraff verkställas i ett annat nordiskt land. Det krävs inte samtycke från den dömda för överförande. Inte heller krävs dubbel straffbarhet. För verkställighet av bötesstraff eller förverkande ställs inget krav på medborgarskap eller hemvist.

Verkställighet i Sverige sker enligt svensk lagstiftning.

Den nordiska verkställighetslagen bygger på direktkontakt mellan de behöriga myndigheterna i respektive stat och på att den rättsliga prövningen görs av dessa myndigheter. I Sverige svarar Kriminalvården både för framställningar om överförande och för beslut om verkställigheten av en påföljd ska ske i Sverige. I fråga om bötesstraff beslutar Kronofogdemyndigheten.

5.5.5 Övertagande av straffverkställighet till följd av en arresteringsorder

Enligt lagen om en europeisk arresteringsorder (se avsnitt 5.4.2) kan en annan stats begäran om överlämnade avslås i vissa fall. Om domstolen har avslagit en begäran om överförande till en annan stat för verkställighet av en frihetsberövande påföljd därför att den som söks för verkställigheten är svensk medborgare

och begär denne att påföljden ska verkställas i Sverige, ska Sverige överta verkställigheten, om inte den andra staten motsätter sig det (2 kap. 6 § och 7 kap. 1 § lagen om överlämnande från Sverige enligt en europeisk arresteringsorder).

5.5.6 Straffverkställighet i Sverige av straff utdömda av internationella tribunaler och domstolar

Sverige har ingått straffverkställighetsavtal med Internationella brottmålstribunalen för f.d. Jugoslavien, Internationella brottmålstribunalen för Rwanda och Specialdomstolen för Sierra Leone (SÖ 1999:25, 2004:17 och 2006:10). Enligt lagen (1994:569) om samarbete med de internationella tribunalerna för brott mot internationell humanitär rätt och lagen (2006:615) om samarbete med Specialdomstolen för Sierra Leone får regeringen besluta att fängelse domar meddelade av dessa internationella domstolar verkställs i Sverige. I Romstadgan för Internationella brottmålsdomstolen, som Sverige tillträdde år 2001, (SÖ 2002:59) finns också regler om verkställighet av straff. Dessa har genomförts i svensk rätt genom lagen (2002:329) om samarbete med Internationella brottmålsdomstolen.

5.5.7 Samarbete rörande kriminalvård i frihet

Lagen om internationellt samarbete rörande kriminalvård i frihet

En annan lag reglerar på motsvarande sätt samarbetet rörande icke frihetsberövande påföljder, lagen (1978:801) om internationellt samarbete rörande kriminalvård i frihet. Lagen bygger på den europeiska konventionen den 30 november 1964 rörande övervakning av villkorligt dömda eller villkorligt frigivna personer och omfattar endast samarbete med sådana stater som har tillträtt konventionen (1 §). Om det finns synnerliga skäl kan

dock regeringen för ett enskilt fall besluta att samarbete ska äga rum även med en stat som inte har tillträtt konventionen.

Samarbetet omfattar, såvitt gäller verkställighet i Sverige,

- utländsk brottmålsdom varigenom den dömda fått villkorligt anstånd med ådömande av straff eller med verkställighet av frihetsstraff eller på annat liknande sätt ålagts att under en provotid undergå kriminalvård i frihet, och
- utländsk frihetsberövande påföljd sedan den dömda enligt beslut i den andra staten har frigetts villkorligt eller annars överförts till kriminalvård utom anstalt.

När det gäller svensk dom som ska verkställas i en annan stat omfattar lagen

- dom på skyddstillsyn, och
- dom på fängelse, sedan den dömda enligt beslut här i landet har frigetts villkorligt.

Bestämmelserna om förfarandet liknar de som gäller enligt brottmålsdomskonventionen.

Rambeslut om erkännande och övervakning av uppskjutna, alternativa och villkorliga påföljder

I januari 2007 presenterade Tyskland och Frankrike ett förslag till rambeslut om erkännande och övervakning av uppskjutna, alternativa och villkorliga påföljder mellan medlemsstaterna inom Europeiska unionen. Rambeslutet syftar till att förbättra samarbetet mellan medlemsstaterna i de fall där en person har dömts till en icke frihetsberövande påföljd i en medlemsstat men har sin hemvist i en annan medlemsstat. Vid ministerrådets för rättsliga och inrikes frågor möte den 6–7 december 2007 nåddes en principöverenskommelse om innehållet i rambeslutet.

Syftet med rambeslutet är att öka den dömdes möjlighet till social återanpassning genom att vederbörande får verkställa påföljden i den stat där han eller hon vistas. Enligt förslaget ska den stat där personen har sin hemvist vara skyldig att överta verkställigheten av den uppskjutna, alternativa eller villkorliga påfölj-

den, förutsatt att ingen av de vägransgrunder som anges i förslaget är tillämplig.

De påföljder som omfattas av förslaget är icke frihetsberövande påföljder där den dömde förutsätts att leva upp till vissa uppställda villkor under viss tid, t.ex. skyddstillsyn. Rambeslutet är även tillämpligt på villkorlig frigivning. Det innehåller närmare bestämmelser om vilka typer av föreskrifter som ska kunna övervakas, t.ex. föreskrifter beträffande bostadsort, utbildning eller yrkesverksamhet. Mot bakgrund av de stora skillnaderna i staternas påföljdssystem har den verkställande staten viss möjlighet att anpassa påföljden till den egna lagstiftningen.

5.6 Samarbetet med vissa internationella organ

5.6.1 Interpol

ICPO – Interpol, som grundades år 1923, är en mellanstatlig organisation för polissamarbete som vilar på folkrättslig grund. Sverige blev medlem år 1926. Förenta nationerna har accepterat Interpols verksamhet och status och organisationen har ett representationskontor vid Förenta Nationernas högkvarter. Interpols syfte är att underlätta gränsöverskridande polissamarbete. Interpol fungerar som länk även i de fall där det inte finns diplomatiska förbindelser mellan staterna. Organisationen har sitt huvudkontor i Lyon i Frankrike. Interpol fungerar främst som ett kontaktorgan mellan de stater som är medlemmar i organisationen och som en kanal för att sprida polisiär information till ett flertal länder.

Interpol för olika databaser för gemensamma ändamål, exempelvis ett internationellt register över stulna motorfordon. Organisationen erbjuder också medlemsstaterna hjälp med kunskap och information om metodutveckling samt arrangerar utbildningar för polismän.

För närvarande är 186 länder medlemmar i Interpol. Varje medlemsland har en nationell Interpolbyrå, som är utpekad som

kontaktpunkt både i förhållande till Interpol och till medlemsländerna i deras inbördes kontakter. I Sverige finns den nationella byrån vid Rikskriminalpolisen.

Samarbetet inom Interpol styrs av medlemsländernas lagstiftningar. Interpol fungerar inte bara som ett organ för polisiärt samarbete utan medverkar även vid rättslig hjälp och bistår på begäran andra myndigheter än polisen, bl.a. åklagare, Tullverket och Kriminalvården. Det finns inte någon särskild rättslig reglering av samarbetet med Interpol. Information lämnas till Interpol med stöd av reglerna i polisens registerlagstiftning, framför allt polisdatalagen och lagarna om belastningsregister och misstankeregister.

5.6.2 Europol

Den europeiska polisbyrån, Europol, upprättades år 1995 genom Europolkonventionen. Sverige godkände konventionen år 1997 (prop. 1996/97:164). Verksamheten vid Europol inleddes år 1999. Sedan dess har vissa ändringar och utvidgningar skett, bl.a. av mandatet, tillgången till Europols information samt Europols deltagande i gemensamma utredningsgrupper genom tre olika tilläggsprotokoll till konventionen som trätt i kraft under våren 2007. Europol verkar inom ramen för det mellanstatliga brottsbekämpande samarbetet inom Europeiska unionen.

Europols främsta uppgift är att vara ett kriminalunderrättelseorgan för medlemsstaterna inom Europeiska unionen. Som sådan ska Europol vara en knutpunkt för utbyte av information och underrättelser mellan medlemsstaterna, vilka tillhandahåller Europol uppgifter bl.a. ur sina polisregister. Dessa uppgifter sammanställs och bearbetas samt kompletteras ibland med uppgifter från annat håll och analyseras hos Europol. Underrättelserna går sedan tillbaka till medlemsstaternas behöriga myndigheter, som härigenom får ett bättre underlag för sin operativa verksamhet.

Tanken är att arbetet ska bidra till fler ingripanden mot den typ av brottslighet som ingår i Europols uppdrag, vilket är organiserad internationell kriminalitet av allvarligt slag, främst narkotikahandel men också annan grov brottslighet. De brott som ingår i Europols uppdrag definieras i konventionen och tilläggsprotokoll till denna. Listan på brott kan utökas genom enhälliga beslut av rådet. Utöver de särskilt definierade brotten kan Europol också anlitas vid penningtvätt som hänger samman med sådana brott och viss annan brottslighet som har anknytning till de brott som ingår i Europols mandat, nämligen brott som begås för att skaffa resurser för att begå brott som tillhör det primära området och brott som begås för att underlätta utförandet eller undgå lagföring för sådana brott.

Inom varje medlemsstat finns en nationell enhet som utgör länken till Europol. Den svenska nationella enheten finns vid Rikskriminalpolisen. Den nationella enheten har till huvudsaklig uppgift att förse Europol med uppgifter. Varje medlemsland sänder dessutom minst en sambandsman till Europols huvudkontor, som ligger i Haag i Nederländerna.

Europol kan tas i anspråk när de faktiska omständigheterna visar att det förekommer en brottslig organisation eller struktur som påverkar två eller flera medlemsstater och som med hänsyn till brottslighetens omfattning, svårhetsgrad och konsekvenser gör det nödvändigt med ett gemensamt handlande från medlemsstaternas sida.

Europol har egna datasystem och upprättar särskilda analysfiler för de ärenden där Europol tar på sig att utföra analysarbetet. Europolkonventionen innehåller detaljerade regler om dataskyddet hos Europol och om tillgång till uppgifter som behandlas av Europol.

Det pågår för närvarande förhandlingar om att omvandla Europolkonventionen till ett rådsbeslut, se avsnitt 7.1

5.6.3 Eurojust

Eurojust, åklagarsamarbetet inom Europeiska unionen, inrättades år 2002. Eurojust har status som EU-organ. Eurojusts huvuduppgifter är att främja och förbättra samordningen mellan medlemsstaternas brottsbekämpande myndigheter vid bekämpningen av grov gränsöverskridande brottslighet. Eurojust ska bl.a. hjälpa medlemsstaterna i frågor om internationell rättslig hjälp och utlämning.

Eurojust består av en nationell medlem från varje medlemsstat. Varje medlem får biträdas av en eller flera personer. Eurojust kan utföra sina uppgifter antingen som ett kollegium eller genom en eller flera nationella medlemmar. De nationella medlemmarna lyder under sin egen stats lagstiftning. Varje medlemsstat avgör själv om den nationella medlemmen ska ha några rättsliga befogenheter i förhållande till sin medlemsstat. Den svenska nationella medlemmen är åklagare.

Eurojust har möjlighet att uppmana rättsliga myndigheter i en medlemsstat som berörs av ett ärende att genomföra brottsutredning och väcka åtal. Eurojust kan vidare uppmana de berörda myndigheterna att samordna utredningar. Eurojust har dock inte några egna rättsliga befogenheter. Beslut i brottsutredningar fattas alltid på nationell nivå, av åklagare, domare eller andra tjänstemän med motsvarande behörighet och med tillämpning av nationell lagstiftning.

Om en behörig myndighet i en medlemsstat inte efterkommer en begäran från Eurojust att inleda en förundersökning eller att väcka åtal, ska Eurojust underrättas om skälen för detta. Det finns vissa undantag från underrättelseskyldigheten, bl.a. om en underrättelse skulle skada viktiga nationella säkerhetsintressen.

För närvarande pågår förhandlingar inom Europeiska unionen om ett nytt rådsbeslut för Eurojust, se avsnitt 7.2.

5.6.4 European Judicial Network

European Judicial Network (EJN) inrättades år 1998 genom en gemensam åtgärd beslutad av Europeiska rådet. EJN består av företrädare för nationella myndigheter (kontaktpunkter) som arbetar med internationellt straffrättsligt samarbete. Kontaktpunkterna är aktiva mellanhänder för att underlätta det rättsliga samarbetet mellan medlemsstaterna när det gäller bekämpandet av framför allt grov brottslighet. Kontaktpunkterna har dagliga kontakter sinsemellan, vanligtvis per telefon eller e-post, i konkreta brottsutredningar. Dessutom träffas kontaktpunkterna ett antal gånger per år för att utbyta erfarenheter och diskutera praktiska och rättsliga problem.

Det pågår för närvarande förhandlingar inom Europeiska unionen om ett nytt rättsligt instrument för EJN, se avsnitt 7.3.

5.6.5 World Customs Organization

Tullverket deltar i samarbetet i Världstullorganisationen (World Customs Organization, WCO), där totalt 171 av världens länder är medlemmar. WCO:s syfte är att förbättra, förenkla och effektivisera arbetet med tullprocedurer inom och mellan medlemsländer. Ursprunget till WCO var principerna i General Agreement on Tariffs and Trade, den s.k. GATT-överenskommelsen.

WCO, som är en mellanfolklig organisation, tillkom år 1952 och har sitt säte i Bryssel i Belgien. WCO:s verksamhet bygger på ett antal internationella konventioner, bl.a. den tidigare nämnda konventionen från år 1977 om ömsesidigt bistånd för att förhindra, utreda och beivra tullbrott (se avsnitt 5.3.2). Det är en multilateral konvention som är relativt allmänt hållen och som kan biträdas av medlemmarna i organisationen om de så önskar. Sverige har enbart accepterat delar av konventionen, bl.a. de delar som rör spontant informationsutbyte avseende misstankar om allvarliga tullbrott, central registrering av uppgifter om

smuggling och ömsesidigt bistånd i kampen mot narkotika (se prop. 1999/2000:122 s. 16).

Arbetet inom WCO bedrivs i s.k. kommittéer. Administrationen består av ett sekretariat som organiserar och leder den dagliga verksamheten.

WCO har inrättat elva regionala underrättelsekontor, varav ett finns i Europa.

6 Förslag till ny lagstiftning om behandling av personuppgifter hos de brottsbekämpande myndigheterna m.m.

6.1 Förslag till ny lag om behandling av personuppgifter i polisens brottsbekämpande verksamhet

Som tidigare nämnts har ett förslag till en helt ny reglering, som ska ersätta polisdatalagen och polisdataförordningen, presenterats i departementspromemorian *Behandling av personuppgifter i polisens brottsbekämpande verksamhet* (Ds 2007:43). Promemorian har remissbehandlats och en proposition planeras till hösten 2008.

6.1.1 Tillämpningsområdet

Lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet ska enligt förslaget gälla vid all behandling av personuppgifter i polisens brottsbekämpande verksamhet vid Rikspolisstyrelsen, polismyndigheterna och Ekobrottsmyndigheten.

Den personuppgiftsbehandling som sker med stöd av de särskilda lagarna om belastningsregister, misstankeregister, Schengens informationssystem samt passagerarregister ska dock inte

omfattas av den nya lagen. Lagen ska inte heller reglera personuppgiftsbehandling i polisens allmänna spaningsregister. Insamling av personuppgifter genom allmän kameraövervakning, hemlig teleavlyssning, hemlig teleövervakning, hemlig kameraövervakning eller hemlig rumsavlyssning undantas också från tillämpningsområdet. För polisens spaningsregister föreslås en särskild lag (se avsnitt 6.1.11).

6.1.2 Grundläggande bestämmelser

Den nya lagen ska enligt förslaget gälla i stället för personuppgiftslagen och förses med hänvisningar till de bestämmelser i personuppgiftslagen som ska gälla vid behandling av personuppgifter i polisens brottsbekämpande verksamhet.

I lagen anges uttömmande för vilka ändamål behandling av personuppgifter får ske. Uppgifter ska således inte få behandlas för några andra ändamål.

De *primära ändamålen* är tre. För det första får personuppgifter behandlas i polisens brottsbekämpande verksamhet om det behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet. För det andra får sådana uppgifter behandlas om det behövs för att utreda och beivra brott. För det tredje får behandling ske om det krävs för att fullgöra ett internationellt åtagande.

Personuppgifter ska dessutom alltid få behandlas om behandlingen är nödvändig för diarieföring eller om uppgifterna har lämnats i en anmälan eller liknande och behandlingen är nödvändig för handläggningen.

I lagens anges också för vilka *sekundära ändamål* uppgifter får behandlas i polisens brottsbekämpande verksamhet. Behandling är tillåten om den är nödvändig för att tillhandahålla information som behövs i

1. brottsbekämpande verksamhet hos Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket,

2. brottsbekämpande verksamhet hos en utländsk myndighet eller mellanfolklig organisation,
3. annan verksamhet som polisen ansvarar för, om det finns särskilda skäl, eller
4. annan myndighets verksamhet, om det enligt lag eller förordning åligger polisen att bistå myndigheten med viss uppgift.

Uppgifterna får slutligen även behandlas om det är nödvändigt för att tillhandahålla information till riksdagen och regeringen samt till andra, om uppgiftsskyldighet följer av lag eller förordning.

Tillgången till personuppgifter ska alltid begränsas till vad varje tjänsteman behöver för att fullgöra sina arbetsuppgifter. En myndighet som har direktåtkomst till personuppgifter ska ansvara för att tillgången begränsas på det sättet.

Rikspolisstyrelsen och polismyndigheterna ska vara personuppgiftsansvariga för den behandling av personuppgifter som myndigheterna utför.

6.1.3 Gemensamt tillgängliga uppgifter

I stället för bestämmelser om register och databaser ska den nya lagen innehålla särskilda bestämmelser om behandling av uppgifter som görs eller har gjorts gemensamt tillgängliga i den brottsbekämpande verksamheten. Regleringen tar framför allt sikte på sådan behandling av uppgifter som sker i för verksamheten gemensamma uppgiftssamlingar. Behandling som utförs av en enskild tjänsteman eller inom en begränsad grupp personer, t.ex. genom vanlig ordbehandling eller genom e-postkommunikation mellan ett fåtal tjänstemän, ska inte omfattas av dessa bestämmelser. Registerbegreppet behålls för vissa särskilda fall.

I förslaget anges olika begränsningar för vilka uppgifter som får göras gemensamt tillgängliga.

I verksamhet som avser att *förebygga, förhindra och upptäcka brottslig verksamhet* ska enbart följande personuppgifter få göras gemensamt tillgängliga.

1. Uppgifter som kan antas ha samband med misstänkt brottslig verksamhet som
 - a) innefattar brott för vilket är föreskrivet fängelse i ett år eller däröver eller
 - b) sker systematiskt.
2. Uppgifter som behövs för övervakningen av personer som
 - c) a) kan antas komma att begå brott för vilket är föreskrivet fängelse i två år eller däröver och
 - d) b) är allvarligt kriminellt belastade eller kan antas vara farliga för annans personliga säkerhet.

Information om att en person är föremål för övervakning ska få göras tillgänglig för flera medan tillgången till uppgifter enligt punkten 2 i övrigt begränsas.

Personuppgifter som förekommer i ärenden om *utredning och beivrande av brott* ska alltid få göras gemensamt tillgängliga. Detta ska dock inte gälla DNA-profiler.

Uppgifter som har *rapporterats till polisens kommunikationscentraler* får också göras gemensamt tillgängliga.

Uppgifter i *det internationella samarbetet* får göras gemensamt tillgängliga om det behövs för att fullgöra den aktuella förpliktelsen.

Personuppgifter som görs eller har gjorts gemensamt tillgängliga ska förses med en särskild upplysning om det närmare ändamålet med behandlingen. De ska vidare förses med en särskild upplysning om att personen som uppgiften avser inte är misstänkt, om de direkt kan hänföras till en sådan person.

Uppgifter, som avser en person som kan antas ha samband med misstänkt brottslig verksamhet, ska förses med upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. Detsamma gäller för personuppgifter som behandlas inom ramen för övervakning av brottsmisstänkta personer.

6.1.4 Sökbegränsningar

Av integritetsskäl ska olika begränsningar gälla för behandlingen. Känsliga personuppgifter ska inte få användas som sökbegrepp vid sökning i gemensamt tillgängliga uppgifter. Det ska dock inte finnas något hinder mot att använda uppgifter som beskriver en persons utseende som sökbegrepp.

Vid sökning i gemensamt tillgängliga uppgifter på namn, firma, personnummer, samordningsnummer, organisationsnummer eller andra liknande identitetsbeteckningar, får enligt huvudregeln endast sådana uppgifter tas fram som anger att den sökta personen

- är anmäld för brott eller är misstänkt för brott eller för brottslig verksamhet,
- övervakas på grund av allvarlig kriminell belastning eller befarad farlighet för annans personliga säkerhet,
- har anmält ett brott eller är målsägande i ett ärende,
- är vittne eller annars ska höras eller avge yttrande i ett ärende,
- har gett in eller tillsänts en handling, eller
- är anmäld försvunnen.

Dessa begränsningar ska dock inte gälla vid sökning som sker i en viss handling eller i ett visst ärende. De ska inte heller gälla vid sökning i en uppgiftssamling som har skapats för att undersöka vissa preciserade slag av brottslighet eller vissa preciserade kriminella grupperingar och som enbart de som arbetar i undersökningen eller vissa särskilt angivna tjänstemän har åtkomst till.

Begränsningarna ska inte heller gälla vid sökning som sker för att förebygga, förhindra eller upptäcka särskilt allvarlig brottslig verksamhet eller för övervakning av personer som kan antas komma att begå brott och som är allvarligt kriminellt belastade eller kan antas vara farliga för annans personliga säkerhet, om sökningen utförs av särskilt angivna tjänstemän. Begränsningarna ska inte heller gälla för utredning av särskilt allvarliga brott.

6.1.5 Behandling av känsliga personuppgifter

Uppgifter om en person ska inte få behandlas 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, s.k. känsliga personuppgifter (se avsnitt 4.2.5). Uppgifter om en person som behandlas på annan grund ska dock få kompletteras med känsliga personuppgifter, om det är absolut nödvändigt för syftet med behandlingen. Känsliga personuppgifter ska också få behandlas, om detta är nödvändigt för diarieföring eller om uppgifterna har lämnats i en anmälan eller liknande och behandlingen är nödvändig för handläggningen.

6.1.6 Informationsutbyte och sekretess

En effektiv brottsbekämpning förutsätter att de brottsbekämpande myndigheterna kan utbyta information på ett rationellt sätt. Det internationella utbytet av information spelar en viktig roll för bekämpningen av allvarlig och gränsöverskridande brottslighet. Det arbetet bör enligt förslaget kunna bedrivas i huvudsak på samma sätt som hittills.

Vidare konstateras att samtliga brottsbekämpande myndigheter i olika avseenden har behov av att kunna få direktåtkomst till vissa typer av uppgifter som behandlas av polisen. Av det skälet föreslås regler för dels i vilken utsträckning polismyndigheterna ska kunna få direktåtkomst till varandras uppgifter, dels i vilken utsträckning andra brottsbekämpande myndigheter ska kunna få direktåtkomst till uppgifter hos polisen. Ett villkor för direktåtkomst är att uppgifterna har gjorts gemensamt tillgängliga.

Regeringen föreslås få meddela föreskrifter om att utländska myndigheter får medges direktåtkomst till uppgifter i polisens brottsbekämpande verksamhet, om det är nödvändigt för att fullgöra förpliktelser som följer av en internationell överenskommelse som har godkänts av riksdagen.

Det krävs sekretessbrytande regler för att skapa förutsättningar för en myndighet att medge andra brottsbekämpande myndigheter direktåtkomst. I promemorian föreslås att uppgifter som har gjorts gemensamt tillgängliga hos den öppna polisen, utan hinder av sekretess enligt 7 kap. 1 a § och 9 kap. 17 § sekretesslagen, ska kunna lämnas till en *annan brottsbekämpande svensk myndighet*, om denna behöver uppgiften i sin brottsbekämpande verksamhet. För uppgifter om resultat av DNA-analyser föreslås särskilda regler.

Personuppgifter ska vidare få lämnas till en *utländsk myndighet eller mellanfolklig organisation*, om det följer av en internationell överenskommelse som Sverige efter riksdagens godkännande har tillträtt. Enligt förslaget ska uppgifter vidare, om det är förenligt med svenska intressen, få lämnas

- till en polis- eller åklagarmyndighet i en stat som är ansluten till Interpol, eller till organisationerna Interpol eller Europol, om det behövs för att myndigheten eller organisationen ska kunna förebygga, upptäcka, utreda eller beivra brott, eller
- till en utländsk underrättelse- eller säkerhetstjänst.

Rätten att lämna uppgifter till utländsk myndighet eller organisation motsvarar i sak vad som gäller i dag.

Endast enstaka personuppgifter föreslås få lämnas ut på medium för automatiserad behandling, om inte regeringen har meddelat avvikande föreskrifter eller i ett enskilt fall har beslutat om att uppgifter får lämnas ut på sådant medium.

6.1.7 Gallring

I promemorian föreslås olika gallringsregler beroende på om en uppgift har gjorts gemensamt tillgänglig eller inte. Personuppgifter som *inte har gjorts gemensamt tillgängliga* ska gallras senast ett år från det att de behandlades automatiserat första gången eller, om de har behandlats inom ett ärende, senast ett år från det att ärendet avslutades.

Personuppgifter som *har gjorts gemensamt tillgängliga* och som kan antas ha samband med brottslig verksamhet ska gallras senast tre år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes. Om den person som en uppgift avser inte är eller har varit misstänkt, ska uppgiften gallras senast tre år efter det att den behandlades automatiserat första gången.

Uppgifter som har behandlats i samband med *övervakning av brottsbelastade eller potentiellt farliga personer* ska gallras senast tio år efter utgången av det kalenderår då den senaste registreringen avseende den övervakade gjordes. Om en uppgift inte avser den övervakade personen, ska uppgiften gallras senast tre år efter det att den behandlades automatiserat första gången.

Den tid under vilken en person avtjänar ett fängelsestraff eller genomgår sluten ungdomsvård eller rättspsykiatrisk vård med särskild utskrivningsprövning ska inte räknas med vid beräkningen av respektive gallringsfrist.

Uppgifter som har behandlats inom ramen för *internationellt samarbete* ska gallras senast ett år efter det att ärendet i vilket uppgifterna behandlades avslutades.

Uppgifter som har rapporterats till polisens *kommunikationscentraler* ska gallras senast ett år efter rapporteringen.

Det införs inte några särskilda gallringsbestämmelser för uppgifter i brottsanmälningar, förundersökningar och andra utredningar som handläggs enligt bestämmelser i 23 kap. rättegångsbalken. Liksom i dag ska sådana uppgifter gallras enligt bestämmelserna i arkivlagen (1990:782). Det föreslås dock vissa begränsningar i möjligheten att använda uppgifterna i brottsbekämpningen efter det att ärendena har avslutats.

6.1.8 Särskilda register

Några få register, för vilka Rikspolisstyrelsen är personuppgiftsansvarig, särregleras även i den föreslagna lagen.

Det föreslås särskilda bestämmelser om register med uppgifter om resultat av DNA-analyser. I lagen införs också särskilda bestämmelser om fingeravtrycksregister, signalementsregister och penningtvättsregister. Några särskilda bestämmelser om andra register som förs hos polisen föreslås inte. Det allmänna spaningsregistret ska, som tidigare nämnts, regleras i en särskild lag. De nuvarande bestämmelserna om DNA-register överförs i huvudsak oförändrade till den nya lagen. Uppgifter om resultat av DNA-analyser får dock enligt förslaget behandlas även för att underlätta identifiering av avlidna personer.

Bestämmelserna i polisdatalagen om ändamålet med och innehållet i fingeravtrycks- och signalementsregister förs i huvudsak oförändrade över till den nya lagen. Dessa register får dock i fortsättningen innehålla även uppgifter om brottskoder.

En nyhet är att Finanspolisens register över ärenden om misstänkt penningtvätt regleras särskilt. I registret får behandlas uppgifter för att förebygga, förhindra och upptäcka brottslig verksamhet

- där penningtvätt ingår som ett led för att dölja vinning av brott eller brottslig verksamhet, eller
- som innefattar brott enligt 3 § lagen (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall, m.m.

I den nya lagen föreskrivs särskilda regler om gallring av uppgifter i de register som särregleras.

6.1.9 Särskilda bestämmelser för Säkerhetspolisen

Särdragen i Säkerhetspolisens verksamhet motiverar enligt promemorian att det i den nya lagen införs särskilda bestämmelser för behandlingen av personuppgifter i Säkerhetspolisens brottsbekämpande verksamhet. Regleringen bör i huvudsak ha samma innebörd som i dag, men bestämmelserna om det s.k. SÄPO-registret föreslås utgå.

Många av de bestämmelser som föreslås gälla i polisens brottsbekämpande verksamhet i övrigt ska gälla även i Säkerhetspolisens verksamhet, däribland bestämmelserna om

- förhållandet till personuppgiftslagen,
- behandlingen av känsliga personuppgifter,
- tillgången till uppgifter och
- utlämnande av uppgifter till bl.a. utländsk myndighet.

Vidare ska bestämmelser med i huvudsak samma innebörd som motsvarande bestämmelser för polisen i övrigt gälla i fråga om behandling av uppgifter om juridiska personer och personuppgiftsansvar.

I lagen anges uttömmande för vilka ändamål Säkerhetspolisen får behandla personuppgifter i den brottsbekämpande verksamheten. På samma sätt som för den övriga polisen anges primära och sekundära ändamål för behandlingen, men de skiljer sig på några punkter från vad som gäller för denna.

Säkerhetspolisen får enligt förslaget behandla personuppgifter endast om det behövs för att

- förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott mot rikets säkerhet, terroristbrott samt vissa yttrandefrihetsbrott och tryckfrihetsbrott,
- utreda eller beivra sådana brott, eller, efter särskilt beslut, annat brott,
- fullgöra bevaknings- och säkerhetsarbete avseende personskydd,
- fullgöra uppgifter enligt säkerhetsskyddslagen (1996:627),
- fullgöra de förpliktelser som följer av internationella åtaganden och
- lämna tekniskt biträde till vissa andra brottsbekämpande myndigheter.

Om Säkerhetspolisen behandlar personuppgifter med stöd av något av de primära ändamålen, får uppgifterna även behandlas när det är nödvändigt för att tillhandahålla information till andra myndigheter och organ enligt i huvudsak samma principer som ska gälla för polisen i övrigt.

På samma sätt som för polisen i övrigt görs skillnad mellan uppgifter som är gemensamt tillgängliga och uppgifter som bara är tillgängliga för en mindre krets. För gemensamt tillgängliga uppgifter ska, på samma sätt som för polisen i övrigt, särskilda sökbegränsningar gälla.

För säkerhetspolisen föreslås särskilda gallringsregler. Personuppgifter som har gjorts gemensamt tillgängliga ska gallras senast tio år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes. Beträffande gallring av uppgifter som inte har gjorts gemensamt tillgängliga föreslås samma regler som för polisen i övrigt.

Personuppgifter som behandlas i en s.k. analysdatabas ska gallras senast tre år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes.

Säkerhetspolisen får besluta att personuppgifter får behandlas under längre tid än vad som nu har sagts, om uppgifterna fortfarande behövs för det ändamål för vilket de behandlas. Ett sådant beslut ska omprövas inom tre år.

På samma sätt som föreslås för polisen i övrigt ska bestämmelserna om gallring inte tillämpas på uppgifter i brottsanmälningar, förundersökningar eller andra utredningar som handläggs enligt bestämmelser i 23 kap. rättegångsbalken. För behandling av uppgifter i avslutade förundersökningar ska också samma bestämmelser gälla som i den övriga polisens verksamhet.

6.1.10 Tillsyn

Datainspektionen ska enligt förslaget utöva tillsyn över all behandling av personuppgifter som polisen utför inom den brottsbekämpande verksamheten.

Personuppgiftsbehandlingen hos Säkerhetspolisen och behandlingen av känsliga personuppgifter inom hela polisen ska dessutom stå under tillsyn av Säkerhets- och integritetsskyddsnämnden. Nämnden, som tillkom den 1 januari 2008, har som huvuduppgift att utöva tillsyn över brottsbekämpande myndig-

heters användning av hemliga tvångsmedel och kvalificerade skyddsidentiteter (se prop. 2006/07:133 s. 61 ff.).

6.1.11 Förslag till lag om polisens spaningsregister

I departementspromemorian läggs också fram förslag till en särskild lag om polisens spaningsregister. Polisen behöver enligt promemorian även i fortsättningen kunna anteckna sådana uppgifter som i dag finns i det allmänna spaningsregistret. Den nya lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet förväntas på sikt tillgodose de behov som det allmänna spaningsregistret fyller, men under en övergångstid bör det allmänna spaningsregistret bibehållas med stöd av en särskild författningsreglering.

Registret ska enligt förslaget regleras i en särskild lag med begränsad giltighetstid. Den ska ge möjlighet att registrera i huvudsak samma uppgifter som i dag. Registret ska föras av Rikspolisstyrelsen, som också ska vara personuppgiftsansvarig.

Lagen, som ska gälla vid sidan av personuppgiftslagen, ska enligt förslaget uttömmande reglera vad som gäller för det allmänna spaningsregistret. Ändamålet med registret ska vara att underlätta tillgången till personuppgifter som behövs för spaning i polisens brottsbekämpande verksamhet. Lagen ska innehålla bestämmelser om vilka kategorier av uppgifter som får behandlas.

Uppgifter som kan hänföras till en enskild person ska som huvudregel få behandlas endast om

- den som uppgiften avser kan misstänkas ha begått ett brott, som inte enbart har böter i straffskalan, och
- behandlingen är av särskild betydelse för brottsbekämpningen.

Även uppgifter som kan hänföras till personer som inte kan misstänkas för brott ska dock få behandlas om uppgiften har samband med en misstänkt person och uppgiften har särskild betydelse för polisens spaningsverksamhet.

Därutöver ska uppgifter om en juridisk person, ett transportmedel eller annat föremål som kan antas ha samband med ett brott få behandlas, om behandlingen är av särskild betydelse för brottsbekämpningen, men inte om brottet enbart har böter i straffskalan.

I den föreslagna lagen anges uttömmande vilka typer av uppgifter som får registreras.

En regel om begränsningar i fråga om behandling av känsliga personuppgifter, som motsvarar vad som gäller för den brottsbekämpande verksamheten i övrigt, föreslås.

Uppgifter, som direkt kan hänföras till en person som inte misstänks för brott, ska enligt förslaget föras med en särskild upplysning om detta. Detsamma gäller uppgifter om en juridisk person eller ett transportmedel som indirekt kan hänföras till en sådan person. Någon upplysning behöver dock inte lämnas om det ändå framgår tydligt av omständigheterna att personen inte är misstänkt. Uppgifter som direkt kan hänföras till en person som inte är misstänkt för brott får inte vara sökbara i registret.

I fråga om utlämnande av uppgifter föreslås regler med i huvudsak samma innehåll som finns i förslaget till lag om behandling av personuppgifter i polisens brottsbekämpande verksamhet. Vissa brottsbekämpande myndigheter ska kunna medges direktåtkomst till registret. Som huvudregel ska endast enstaka uppgifter få lämnas ut på medium för automatiserad behandling.

Särskilda gallringsregler föreslås för uppgifter i registret.

Bestämmelserna i personuppgiftslagen om rättelse och skadestånd ska enligt förslaget gälla för behandling i registret.

6.1.12 Ikraftträdande

Både lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet och lagen om polisens spaningsregister föreslås träda i kraft den 1 januari 2009. I fråga om vissa bestämmelser i den förstnämnda lagen föreslås dock en tvåårig övergångsperiod, räknat från ikraftträdandet. De register som

förs med stöd av datalagen och övergångsbestämmelserna till polisdatalagen, liksom andra register som förs med stöd av äldre bestämmelser får enligt förslaget inte längre föras när övergångstiden har löpt ut. Övergångsbestämmelserna till den nuvarande polisdatalagen gäller till utgången av år 2008.

6.2 Förslag till ny lagstiftning om Schengens informationssystem

I avsnitt 4.4.6 finns en kort redogörelse för Schengens informationssystem (SIS). Inom Europeiska unionen har upprättats ett utkast till rådsbeslut om inrättande, drift och användning av andra generationen av SIS. Riksdagen har godkänt rådsbeslutet (prop. 2006/07:33, bet. 2006/07:JuU3), som antogs av rådet den 12 juni 2007.

Det viktigaste skälet till att ett utkast till rådsbeslut togs fram var att det nuvarande systemet anses vara tekniskt föråldrat och inte ha tillräcklig kapacitet för att möta kommande behov. Propositionen, som är en s.k. godkännandeproposition, innehåller inte några lagförslag.

Rådsbeslutet innehåller, såvitt nu är av intresse, regler om skydd för enskilda (artiklarna 56–63) i bl.a. följande hänseenden:

- förbud mot behandling av känsliga personuppgifter,
- bestämmelser om enskildas rätt att få tillgång till uppgifter om sig själva,
- rätten att få oriktiga uppgifter rättade och olagligt lagrade uppgifter raderade,
- regler om rättsmedel, och
- regler om tillsyn.

Dessa delar av utkastet till rådsbeslut motsvarar till stora delar vad som redan gäller enligt Schengenkonventionen. I propositionen görs därför bedömningen att de regler som finns i lagen om Schengens informationssystem, tillsammans med de allmänna reglerna i personuppgiftslagen, innebär att det, utom på någon enstaka punkt, inte krävs några lagändringar i dessa delar.

I artiklarna 54 och 55 föreskrivs begränsningar i rätten att överföra eller göra uppgifter tillgängliga till tredje land och internationella organisationer. Dessa begränsningar bedöms kräva viss lagändring.

Inom Regeringskansliet pågår för närvarande arbetet med att ta fram förslag till nödvändiga lagändringar.

6.3 Genomförande av Prümrådsbeslutet

Den 27 maj 2005 ingick Belgien, Tyskland, Spanien, Frankrike, Luxemburg, Nederländerna och Österrike en konvention i den tyska orten Prüm, den s.k. Prümkonventionen. Konventionsstaternas uttalade målsättning är att utveckla informationsutbytet inom hela Europeiska unionen, framför allt vad gäller DNA-, fingeravtrycks- och fordonsregisteruppgifter.

Eftersom det fanns intresse av att omvandla konventionens bestämmelser till ett eller flera instrument inom ramen för Europeiska unionens regelverk nåddes den 15 februari 2007 en politisk principöverenskommelse om att integrera merparten av Prümfördragets tredjepelarfrågor i unionens regelverk. Därefter har ett förslag till rådsbeslut utarbetats; rådets beslut om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet ("Prümrådsbeslutet"). Vid ett möte i rådet för rättsliga och inrikes frågor den 12 och 13 juni 2007 träffades en politisk överenskommelse om texten i förslaget.

Utgångspunkten för det informationsutbyte som regleras i Prümrådsbeslutet är att man ska utnyttja medlemsstaternas befintliga databaser i stället för att skapa nya. Medlemsstaterna ska automatiskt ges tillgång till varandras DNA-, fingeravtrycks- och fordonsregister i form av begränsad åtkomst till vissa uppgifter. Sådana uppgifter utbyts redan i dag, men sättet att utbyta uppgifter förenklas. Vid automatisk sökning i DNA- och fingeravtrycksregister ska den behöriga myndigheten i en annan stat enbart få uppgift om huruvida det finns uppgifter eller inte (s.k.

hit/no hit-system). Vid automatisk sökning i fordonsregistret ska dels uppgifter om ägare och innehavare av ett fordon, dels uppgifter om fordonet vara tillgängliga.

Rådsbeslutet reglerar också utbyte av personuppgifter och annan information inför större evenemang och informationsutbyte för att förebygga terroristbrott. Vidare regleras visst operativt samarbete. Beslutet innehåller också detaljerade dataskyddsbestämmelser kopplade till bestämmelserna om uppgiftsutbyte.

I propositionen Godkännande av Prömrådsbeslutet (prop. 2007/08:83) har regeringen föreslagit att riksdagen ska godkänna utkastet till Prömrådsbeslut. Propositionen innehåller inte några förslag till lagändringar utan redovisar endast, på ett allmänt plan, vilka lagändringar som kan behövas. Redovisningen mynnar ut i att det kan krävas vissa ändringar i befintliga lagregler samt att vissa nya regler kan behöva införas för att täcka de förpliktelser som följer av rådsbeslutet. Det gäller bl.a. regler om underrättelse om felaktiga uppgifter, om märkning av vissa uppgifter samt gallringsregler. Det rör sig dock inte om något omfattande lagstiftningsbehov.

6.4 VIS

Inom Europeiska unionen pågår också utveckling av informationsutbytet rörande viseringsfrågor. Rådet för rättsliga och inrikes frågor antog den 19 februari 2004 slutsatser om utveckling av ett informationssystem för viseringar. Den 8 juni 2004 beslutade rådet att inrätta informationssystemet för viseringar (VIS) som ett system för utbyte av viseringsuppgifter mellan medlemsstaterna. VIS är således avsett att bli ett gemensamt informationssystem för viseringar inom hela unionen. Det centrala systemet ska ligga i Strasbourg i Frankrike. Det ska vara anslutet till de nationella systemen i varje medlemsstat via s.k. nationella gränssnitt.

Kommissionen presenterade den 28 december 2004 ett förslag till Europaparlamentets och rådets förordning om informations-

systemet för viseringar (VIS) och utbytet av uppgifter mellan medlemsstater om viseringar för kortare vistelser (VIS-förordningen). VIS-förordningen ska antas av Europaparlamentet och rådet gemensamt genom s.k. medbeslutandeförfarande. Medlemsstaterna nådde en politisk överenskommelse om förordningsförslaget i maj 2007. Europaparlamentet har därefter antagit ett betänkande med förslag till ändringar i kommissionens förordningsförslag.

Enligt VIS-förordningen ska VIS ha till syfte att förbättra genomförandet av den gemensamma viseringspolitiken, det konsulära samarbetet och samrådet mellan medlemsstaternas centrala viseringsmyndigheter genom att underlätta utbytet av viseringsuppgifter mellan medlemsstaterna. Ett förenklat utbyte av uppgifter ska bl.a. underlätta hanteringen av viseringsansökningar, gränskontroller och inre utlänningskontroll, men också bidra till att förebygga hot mot medlemsstaternas inre säkerhet.

I mars 2005 antog rådet slutsatser med anledning av bombdåden i Madrid och London enligt vilka det skulle förbättra den inre säkerheten och kampen mot terrorism om myndigheter med ansvar för inre säkerhet ges tillgång till VIS för att ”förhindra och upptäcka straffbara gärningar och utreda sådana, inbegripet terroristdåd eller terroristhot”. Kommissionen presenterade i november 2005 ett förslag till rådsbeslut, rådets beslut om åtkomst till informationssystemet för viseringar (VIS) för sökningar för medlemsstaternas utsedda myndigheter och för Euro-pol i syfte att förhindra, upptäcka och utreda terroristbrott och andra grova brott. En politisk överenskommelse nåddes vid möte med rådet för rättsliga och inrikes frågor den 12 och 13 juni 2007. Sverige lämnade i samband med det en parlamentarisk granskningsreservation. Rådsbeslutet ska tillämpas först efter det att VIS-förordningen har trätt i kraft och är fullt tillämplig, dvs. sannolikt tidigast från den 29 maj 2009.

I en promemoria med utkast till proposition har föreslagits att riksdagen ska godkänna utkastet till rådsbeslut om VIS. Promemorian innehåller inte några förslag till lagändringar utan redovisar endast, på ett allmänt plan, vilka lagändringar som kan

behövas. Eftersom det inte finns någon motsvarighet till det informationsutbyte som föreslås i rådsbeslutet står det klart att det krävs viss lagstiftning, även om rådsbeslutet till stora delar kan genomföras i förordningsform. En fråga som väcks är om befintliga bestämmelser om användningsbegränsningar är tillräckliga. Vidare anses vissa lagändringar angående gallring vara nödvändiga. När det gäller dataskyddet bedöms att den nuvarande lagstiftningen i huvudsak är tillräcklig och att eventuella kompletterande regler kan ges i förordning. Promemorian har remissbehandlats.

6.5 Rambeslut om förenklat informations- och underrättelseutbyte

Den 18 december 2006 antog Europeiska unionens råd ett rambeslut om förenklat informations- och underrättelseutbyte mellan de brottsbekämpande myndigheterna i Europeiska unionens medlemsstater. Initiativet till rambeslutet togs av Sverige. Syftet med rambeslutet är att lägga fast regler för hur de brottsbekämpande myndigheterna snabbt och enkelt ska kunna utbyta befintlig information och befintliga underrättelser.

Rambeslutet tar alltså inte sikte på bevismaterial utan på uppgifter som underlättar underrättelsearbetet och brottsutredande verksamhet. Information får begäras i syfte att upptäcka, förebygga eller utreda brott.

Brådskande förfrågningar ska i princip kunna besvaras inom åtta timmar, om informationen finns tillgänglig. I fall som inte är brådskande ska svar ges inom en vecka.

Information ska även under vissa förutsättningar lämnas spontant för samma ändamål som kan ligga till grund för en begäran om information. Det spontana uppgiftsutbytet ska dock endast avse uppgifter för förebyggande och utredning av vissa uppräknade brott.

Rambeslutet innehåller också en erinran om att uppgifter ska utbytas med Europol i enlighet med Europolkonventionen.

Information kan utbytas med Europol under samma förutsättningar som gäller för informationsutbyte mellan medlemsstater.

Rambeslutet reglerar också skälen för att vägra lämna information. Dessa är att tillhandahållandet skulle kunna

- skada väsentliga nationella säkerhetsintressen,
- äventyra resultatet av pågående utredning eller underrättelsearbete eller skada enskilda personers säkerhet, eller
- vara uppenbart oproportionerligt eller irrelevant för de syften för vilka informationen begärdes.

Rambeslutet, som ska vara genomfört i december 2008, kommer endast att föranleda förordningsändringar för svensk del.

6.6 Förslag till ny reglering av behandlingen av personuppgifter inom Kustbevakningen

6.6.1 Allmänt om förslaget

Den 21 oktober 2004 tillkallades en särskild utredare med uppdrag att göra en översyn av regleringen av behandlingen av personuppgifter i Kustbevakningens verksamhet. Utredningen antog namnet Utredningen om Kustbevakningens personuppgiftsbehandling. Den 28 februari 2006 överlämnade utredningen betänkandet Kustbevakningens personuppgiftsbehandling Integritet – Effektivitet (SOU 2006:18). Betänkandet har remissbehandlats.

I betänkandet lämnar utredningen förslag till en ny lag om behandling av personuppgifter i Kustbevakningens verksamhet, som föreslås ersätta den nuvarande förordningen (2003:188) om behandling av personuppgifter inom Kustbevakningen. De yttre ramarna för behandlingen av uppgifter i Kustbevakningens verksamhet, som är viktiga från integritetsskyddssynpunkt, slås fast i den nya lagen. Lagen ska enligt förslaget gälla i stället för personuppgiftslagen och innehålla hänvisningar till de bestämmelser i personuppgiftslagen som ska vara tillämpliga i Kustbevakning-

ens verksamhet. Lagen utgår från personuppgiftslagens begrepp och terminologi. I lagen anges för vilka ändamål olika typer av uppgifter får behandlas. Dessa skiljer sig beroende på om det är fråga om brottsbekämpande verksamhet eller annan verksamhet.

Förslaget bygger på tanken att regleringen ska vara teknikneutral. I motsats till den befintliga registerlagstiftningen för andra brottsbekämpande myndigheter utgår förslaget varken från begreppet databas eller register. Däremot görs i den brottsbekämpande verksamheten skillnad mellan uppgifter som endast en mindre krets har tillgång till och uppgifter som är tillgängliga för flera. Lagen innehåller bl.a. bestämmelser om behandling av känsliga personuppgifter och om olika typer av sök begränsningar.

Utredningen föreslår vidare ändringar i sekretesslagen, så att Kustbevakningens brottsbekämpande verksamhet i sekretesshänseende regleras på samma sätt som för övriga brottsbekämpande myndigheter. Utredningen föreslår också en ny bestämmelse om sekretess för uppgift om enskilda affärs- och driftförhållande samt för uppgift ur sjömansregistret. Sekretessen ska gälla i register som förs av Kustbevakningen i dess verksamhet med samordning av civil sjöövervakning och förmedling av civil sjöinformation.

Betänkandet har remissbehandlats.

6.6.2 Den fortsatta handläggningen

Sedan betänkandet remissbehandlats gjordes bedömningen att den fortsatta beredningen av förslaget ska samordnas med beredningen av Polisdatautredningens förslag, i syfte att åstadkomma en mer enhetlig reglering av personuppgiftsbehandlingen hos de brottsbekämpande myndigheterna. I den i avsnitt 6.1 redovisade promemorian *Behandling av personuppgifter i polisens brottsbekämpande verksamhet* finns därför även ett avsnitt som behandlar i vilken utsträckning de principiella överväganden som görs angående polisens behandling av personuppgifter även

bör läggas till grund för den fortsatta beredningen av förslaget till ny reglering av personuppgiftsbehandlingen i Kustbevakningens brottsbekämpande verksamhet (Ds 2007:43 s. 388 ff.).

I promemorian konstateras att en rad frågeställningar är gemensamma för den brottsbekämpande verksamheten hos myndigheterna, bl.a. frågor som rör behandlingen av personuppgifter. Vidare slås fast att det är angeläget att samma grundläggande principer gäller för hur den enskildes integritet ska skyddas och hur avvägningen ska ske i förhållande till verksamhetens effektivitet. En samordning av regleringen av personuppgiftsbehandlingen i den brottsbekämpande verksamheten hos polisen och Kustbevakningen skulle skapa bättre förutsättningar för samarbete mellan myndigheterna och underlätta informationsutbytet mellan dem. Det skulle också innebära att den enskilde lättare kan få överblick över vilka förutsättningar som gäller för behandling av uppgifter om honom eller henne i respektive verksamhet. På samma sätt som för polisens del förslås att insamling av vissa typer av uppgifter, vilka regleras i andra lagar, ska falla utanför tillämpningsområdet för den nya lagstiftningen för Kustbevakningens brottsbekämpande verksamhet. Likaså föreslås den framtida regleringen för denna verksamhet innehålla bestämmelser om behandling av uppgifter om juridiska personer, eftersom sådana uppgifter inte alltid kan skiljas från uppgifter om fysiska personer.

Promemorian innehåller dessutom förslag om ändringar i dels lagen (1998:620) om belastningsregister, dels lagen (1998:621) om misstankeregister. Ändringarna innebär att registren i fråga ska föras även för Kustbevakningens räkning. Vidare föreslås Kustbevakningen få samma rätt till uppgifter ur registren som övriga brottsbekämpande myndigheter. Ändringarna innebär att myndigheten kommer att kunna beviljas direktåtkomst till registren i fråga.

Inom Försvarsdepartementet förbereds en lagrådsremiss som behandlar ny lagstiftning på området.

6.7 Förslag till ny lagstiftning om behandling av personuppgifter inom domstolsväsendet

Regeringen beslutade den 19 oktober 2000 att tillkalla en särskild utredare för att granska regleringen och användningen av personregister och annan behandling av personuppgifter inom domstolsväsendet. Utredningen antog namnet Domstolsdatautredningen. Utredningen avgav den 29 mars 2001 delbetänkandet Domstolarnas register och personuppgiftslagen – En rättslig anpassning (SOU 2001:32) och i december 2001 slutbetänkandet Informationshantering och behandling av uppgifter vid domstolar – En rättslig översyn (SOU 2001:100).

Utgångspunkten är att skapa en lagstiftning för domstolsväsendet som medger att domstolarna i stor omfattning kan använda sig av modern teknik. Lagstiftningen ska både garantera integritetsskyddet för enskilda och möjliggöra effektiviseringar genom teknikanvändning. Lagförslagen utgår från begreppen databas och register.

I betänkandet föreslås att de fyra förordningar som i dag reglerar personuppgiftsbehandlingen inom domstolsväsendet ersätts med lagar. Utredningen har inte ansett det inte möjligt att skapa en enda lag för hela domstolsväsendet, utan föreslår en lag för de allmänna domstolarna, en för de allmänna förvaltningsdomstolarna och en tredje för hyres- och arrendenämnder. Lagarna föreslås gälla i stället för personuppgiftslagen och ska innehålla hänvisningar till personuppgiftslagen i de avseenden som den ska vara tillämplig. Förslagen till lagar innehåller bestämmelser bl.a. om personuppgiftsansvar, behandling av känsliga personuppgifter, gallring, databasens ändamål och innehåll samt om utlämnande, direktåtkomst, sökning m.m. Lagförslagen innehåller också bestämmelser om information till den registrerade, rättelse och skadestånd samt överklagande.

Domstolsdatautredningens slutbetänkande, som har remissbehandlats, ligger till grund för ett arbete med förslag till lagreglering av domstolarnas och nämndernas personuppgiftsbehandling. En departementspromemoria planeras till våren 2008.

6.8 Utredning om ny lagstiftning om behandling av personuppgifter inom åklagarväsendet

Regeringen beslutade den 6 september 2007 direktiv för en översyn av reglerna om personuppgiftsbehandling inom åklagarväsendet (dir. 2007:126). Enligt direktiven ska en särskild utredare se över den behandling av personuppgifter som sker inom åklagarväsendet och som avser brottsutredning, åtal eller andra åtgärder vid brottsbekämpning.

Utgångspunkten för utredningen är att den brottsbekämpande verksamheten ska kunna bedrivas så effektivt som möjligt, samtidigt som enskilda personers integritetsintressen ska tas till vara. Utredaren ska på grundval av en kartläggning av användningen av personuppgifter i åklagarväsendets brottsbekämpande verksamhet identifiera verksamhetsbehoven av personuppgiftsbehandling och de integritetsintressen och övriga intressen som kan beröras av behandlingen. Utredaren ska lägga fram ett fullständigt förslag till författningsreglering. Utgångspunkten för översynen är att grundläggande frågor ska regleras i lag, medan detaljfrågor bör regleras i förordning.

Utredningsuppdraget ska redovisas senast den 30 september 2008.

6.9 Integritetsskyddskommitténs synpunkter och förslag

Integritetsskyddskommittén gjorde i sitt första betänkande, Skyddet för den personliga integriteten (SOU 2007:22), en kartläggning och analys av den nuvarande lagstiftningen ur integritetsskyddssynpunkt. Kommittén riktade kritik mot lagstiftningsarbetet inte minst på brottsbekämpningsområdet (SOU 2007:22, del I, s. 468 ff.).

I sitt slutbetänkande Skyddet för den personliga integriteten (SOU 2008:3) har kommittén föreslagit ett utökat grundlagskydd för hantering av bl.a. personuppgifter. För närvarande

regleras i 2 kap. 3 § regeringsformen enbart skyddet för personlig integritet vid automatisk databehandling. Kommittén anser att skyddet i stället bör utformas så att det gäller för intrång, om det sker i hemlighet eller utan samtycke, som innebär övervakning eller kartläggning av den enskildes personliga förhållanden. När det gäller förfaranden från det allmännas sida som enligt kommittén förtjänar ett utvidgat grundlagsskydd nämns bl.a. hemlig kameraövervakning och hemlig teleövervakning. Även informationsinhämtning i form av fotografering med handmanövrerad kamera bör enligt kommittén i vissa lägen kunna jämföras med övervakning genom fast monterad utrustning och därför förtjäna utökat skydd. Polisens personuppgiftshantering vid underrättelseverksamhet är ett annat exempel som kommittén anser kräver ett utökat grundlagsskydd.

Kommittén föreslår dock inte att all hantering av personuppgifter ska omfattas av det utvidgade grundlagsskyddet. De från integritetssynpunkt viktigaste momenten är enligt kommittén insamling av uppgifter, fastställandet av ändamålen med behandlingen och i vilken utsträckning uppgifter på grund av uppgiftsskyldighet ska lämnas ut till andra för samkörning i register eller av annat skäl. Däremot berörs inte sådan uppgiftsskyldighet som förutsätter en sekretessprövning.

Betänkandet är föremål för remissbehandling.

7 Pågående förhandlingsarbete inom Europeiska unionen

7.1 Europol

I december 2006 enades Europeiska unionens råd om att Europolkonventionen (se avsnitt 5.6.2) ska ersättas med ett rådsbeslut. Förhandlingarna om det närmare innehållet i detta pågår fortfarande. Rådsbeslutet är tänkt att innefatta den nuvarande Europolkonventionen men också att utvidga Europols mandat ytterligare så att detta inte längre knyts till organiserad brottslighet. Syftet med utvidgningen är att underlätta för Europol att stödja medlemsstaterna vid utredningar av gränsöverskridande brottslighet där det inte redan från början står klart att brottsligheten är organiserad.

Förslaget till rådsbeslut innehåller ett särskilt kapitel om dataskydd, där tanken är att regleringen i största möjliga utsträckning ska motsvara skyddet enligt det nu aktuella rambeslutet. Det anses dock vara lämpligast med ett sammanhållet regelsystem som är skraddarsytt för Europols behov. Regleringen av dataskyddet innebär i allt väsentligt att de bestämmelser som finns i Europolkonventionen förs över till rådsbeslutet, samtidigt som de anpassas till rambeslutet. Enligt förslaget ska det också i framtiden finnas särskilda regler bl.a. för de analysdatabaser som Europol använder.

7.2 Eurojust

För närvarande förhandlas ett förslag till reviderat rådsbeslut om Eurojust. Förslaget innebär bl.a. att en nationell medlems mandatperiod inte får understiga fyra år samt att den nationella medlemmen ska ha vissa minimibefogenheter att vidta och besluta om åtgärder i hemlandet. Medlemmen ska bl.a. kunna motta, sända och förbereda verkställighet av framställningar om rättsligt samarbete, t.ex. en europeisk arresteringsorder. Åtgärderna ska dock alltid i första hand vidtas av nationell myndighet. En nationell medlem ska också kunna förbereda och delta i gemensamma utredningsgrupper (se avsnitt 5.6.3). Medlemmarna ska dessutom ha möjlighet att, efter samråd med behörig nationell myndighet i enskilda fall, utfärda och färdigställa framställningar om rättslig hjälp samt besluta om husrannsakan, beslag och kontrollerade leveranser. I brådskande fall ska de nationella medlemmarna kunna besluta om kontrollerade leveranser utan föregående samråd med nationell myndighet.

Vidare föreslås att medlemsstaterna får en direkt skyldighet att förse Eurojust med information som är nödvändig för att Eurojust ska kunna utföra sitt uppdrag. Dessutom föreslås en tydligare skyldighet för de behöriga nationella myndigheterna att informera den nationella medlemmen. Skyldigheten att motivera ett beslut att inte efterkomma en begäran från Eurojust skärps också.

7.3 European Judicial Network

För EJNI föreslås ett nytt rättsligt instrument i form av ett rådsbeslut. Det föreslås att varje stat ska utse en av sina kontaktpunkter till nationell kontaktperson för EJNI. Tanken är att denna person ska få en funktion i det föreslagna nationella systemet för Eurojustsamordning. Kontaktpunkterna ska genomföra utbildningar i rättsligt samarbete för myndigheterna i

sina stater. Vidare ska EJN och Eurojust informera varandra om ärenden som kan beröra det andra organets verksamhetsområde.

7.4 Passagerarregister

Sedan terroristattacken i New York den 11 september 2001 har brottsbekämpande myndigheter i olika länder, framför allt i USA, börjat samla in och systematiskt analysera information om flygpassagerare. Som redovisats i avsnitt 4.4.7 är flygföretag enligt ett EU-direktiv skyldiga att lämna vissa uppgifter om sina passagerare, s.k. PNR-uppgifter (Passenger Name Record). Europeiska kommissionen har utarbetat ett förslag till rambeslut om användning av sådana uppgifter för brottsbekämpande ändamål. Rambeslutet ska ses bl.a. mot bakgrund av att Europeiska unionen under våren 2007 ingick avtal med USA om utbyte av information om sådana uppgifter (jfr 13 a § personuppgiftsförordningen). Ett likartat system föreslås nu införas inom Europeiska unionen.

Kommissionens förslag till rambeslut omfattar endast flygtrafik och bara flygrutter som inleds eller avslutas i tredje land. Insamlingen av uppgifter ska enligt förslaget göras av en särskild nationell enhet. Från enheten ska uppgifter kunna föras över till behöriga myndigheter för vissa specificerade ändamål, t.ex. att identifiera personer som är eller kan antas vara inblandade i terroristbrott eller organiserad brottslighet och för att förse myndigheterna med information om rese mönster.

Förhandlingarna om rambeslutet har påbörjats under våren 2008.

8 Genomförande av rambeslutet

8.1 Inget genomgripande behov av ny lagstiftning

Bedömning: Genomförandet av rambeslutet kräver vissa författningsändringar men inte något omfattande nytt lagstiftningsarbete. Även om den svenska lagstiftningen redan till stora delar är anpassad till de krav på dataskydd som rambeslutet föreskriver finns det skäl att göra en i huvudsak teknisk översyn av flera författningar.

Skälen för bedömningen: Ett antal av bestämmelserna i rambeslutet innehåller förpliktelser för medlemsstaterna. Dessa överensstämmer i många avseenden med förpliktelserna i dataskyddsdirektivet. Eftersom man i svensk lagstiftning har valt att genomföra dataskyddsdirektivet generellt, finns det redan författningar som reglerar personuppgiftsbehandlingen inom de verksamhetsområden som berörs av rambeslutets tillämpningsområde. Man kan lite generaliserat säga att det rör sig om tre olika former av lagstiftning; dels sådana lagar som reglerar ett eller flera enskilda register, dels generella författningar för en viss sektor av samhället (som exempelvis polisdatalagen), som dessutom kan reglera ett eller flera register, och dels personuppgiftslagen som tillämpas helt eller delvis. Alla de författningar som gäller vid sidan av personuppgiftslagen brukar betecknas registerförfattningar. För att förenkla framställningen här används benämningen sektorsförfattningar för polisdatalagen och andra författningar som gäller för ett visst verksamhetsområde.

Det finns exempel på verksamheter där både särbestämmelser för ett visst register, en sektorslag och personuppgiftslagen ska tillämpas samtidigt. Lagstiftningen på området är således mycket komplex. Likväl kan konstateras att – genom att rambeslutet innehåller bestämmelser som i många avseenden liknar de som finns i dataskyddsdirektivet och att detta genomförts också inom de sektorer som påverkas av rambeslutet – den svenska lagstiftningen redan till stora delar är anpassad till de krav på dataskydd som ställs i rambeslutet.

Mot den nu angivna bakgrunden krävs det inte något omfattande nytt lagstiftningsarbete, men vissa ändringar av befintlig lagstiftning kommer att krävas. Vidare måste övervägas om personuppgiftslagen, sett i relation till artiklarna i rambeslutet, ger ett tillräckligt skydd för de för personuppgifter som behandlas i de verksamheter och i de situationer där den är tillämplig.

Förekomsten av ett rambeslut som reglerar behandlingen av personuppgifter inom delar av den offentliga verksamheten som inte omfattas av dataskyddsdirektivet väcker naturligtvis också frågan om det bör införas en generell reglering av samma typ som personuppgiftslagen för detta särskilda område. Det förhållandet att sektorsförfattningarna till stora delar innehåller samma undantag från personuppgiftslagen kan möjligen tala för detta. På sikt kan det vara något som bör övervägas, men inget som krävs för att genomföra rambeslutet.

Något som också måste övervägas är om regleringen som rör personuppgiftsbehandling bör ha lagform, för att skyddet för den enskilde ska kunna anses vara tillfredsställande. För närvarande regleras personuppgiftsbehandlingen inom vissa delar av rättsväsendet endast i förordning. Det finns emellertid redan förslag om att de viktigaste delarna av personuppgiftsbehandlingen i domstolarna och inom Kustbevakningen ska regleras i lag. För åklagarväsendets del pågår en översyn med samma inriktning. Inom flera verksamhetsområden kan man således anta att regleringen inom kort får lagform. Därefter återstår bara något enstaka register som för närvarande regleras i förordning. Såväl regeringen som riksdagen har framhållit att myndighetsregister

med ett stort antal registrerade och ett särskilt känsligt innehåll ska regleras i lag (se prop. 1990/91:60 s. 50 och 1997/98:44 s. 41 samt KU 1990/91:11 s. 11.) Det talar för att viss reglering av personuppgiftsbehandling som hittills skett i förordning i framtiden bör ges lagform. Det bör således i det fortsatta arbetet övervägas om de grundläggande bestämmelserna om personuppgiftsbehandling rörande strafförelägganden respektive förelägganden av ordningsbot bör finnas i lag, medan mer detaljerade bestämmelser kan meddelas i förordning. Vidare finns det skäl att överväga om kriminalvårdens reglering, där centrala kriminalvårdsregistret och säkerhetsregistret enbart regleras i förordning, bör ses över i detta hänseende. Det kan anmärkas att översynen av åklagarväsendets personuppgiftshantering, där en av utgångspunkterna är att de viktigaste frågorna ska regleras i lag, omfattar strafförelägganderegister.

Genom propositionen om offentlighetsprincipen och informationstekniken infördes en ny paragraf, 2 kap. 18 § tryckfrihetsförordningen, där det föreskrivs att grundläggande bestämmelser om hur allmänna handlingar ska bevaras samt om gallring och annat avhändande av sådana handlingar ska meddelas i lag (prop. 2001/02:70). Syftet med bestämmelsen är att betona arkivreglernas betydelse för offentlighetsinsynen enligt 2 kap. tryckfrihetsförordningen. Gallringsbestämmelser ingår således numera i det s.k. obligatoriska lagområdet (a. prop. s. 37). Där emot ska detaljreglering fortfarande kunna ske i förordning eller genom myndighetsföreskrifter (a. prop. s. 39). Gallringen fyller en mycket viktig funktion vid behandling av personuppgifter, eftersom syftet med gallringen är att minska integritetsintrånget. Detta kan ses som ytterligare ett skäl för att särregler om personuppgiftsbehandling bör finnas i lag.

Det kan dock inte hävdas att Sverige inte skulle uppfylla förpliktelserna i rambeslutet genom en förordningsreglering, så länge författningarna i övrigt uppfyller kraven. Att vissa författningar inte har lagform spelar alltså ingen roll i det avseendet.

I de följande avsnitten görs, på ett allmänt plan, en bedömning av lagstiftningsbehovet. I vissa fall kan man förvänta sig att de

problem som finns i dagens lagstiftning kommer att lösas inom kort i andra lagstiftningsärenden. Genomförandet av rambeslutet kommer trots detta att kräva en översyn av i huvudsak teknisk natur av ett flertal författningar.

Vad som komplicerar bedömningen av lagstiftningsbehovet, och gör det särskilt svårt att närmare precisera vilka förändringar som kan krävas, är att det, som redovisats i avsnitt 6, för närvarande pågår översyner och lagstiftningsarbete som rör personuppgiftsbehandlingen hos polisen, åklagarväsendet, Kustbevakningen och domstolarna. Förslagen och översynerna berör såväl personuppgiftsbehandlingen i stort som enskilda registerförfattningar. Detta innebär att en bedömning av lagstiftningsbehovet måste ske med utgångspunkt inte bara i den gällande lagstiftningen utan även med hänsynstagande till de förslag om förändringar som är aktuella. Vidare pågår, som redovisats i avsnitt 7, förhandlingar inom Europeiska unionen om andra instrument som påverkar lagstiftningsbehovet. Det innebär att vissa bedömningar som görs i det följande får betraktas som preliminära.

8.2 Personuppgiftslagen och dess roll

8.2.1 Allmänt om personuppgiftslagen

Vid tillkomsten av personuppgiftslagen fanns det redan en generell lagstiftning som reglerade automatisk databehandling av personregister, nämligen datalagen. Mot den bakgrunden var det naturligt att lagstiftaren valde samma lösning när dataskyddsdirektivet genomfördes i svensk rätt. Trots att det var möjligt att undanta delar av den offentliga verksamheten, bl.a. polisens verksamhet, valde man en generell lagstiftning för i princip all personuppgiftsbehandling. Samtidigt konstaterades att de registerförfattningar som tillskapats för särskilt viktiga eller känsligare register innehöll många preciserade och viktiga bestämmelser som inte rimligen kunde ersättas av en ny generell lag. Man behöll därför strukturen med specialförfattningar för vissa

register (se prop. 1997/98:44 s. 40 f.). För polisväsendets del fanns sedan länge en sådan reglering i lagen (1969:94) om polisregister, med tillhörande förordning, samt i vissa andra registerförfattningar. För andra verksamhetsområden infördes sektorsförfattningar, som reglerar behandlingen av personuppgifter inom en viss myndighet eller sektor av samhället. Lagstiftaren föredrog nämligen att ha särregler i särskilda författningar framför att göra generella undantag från personuppgiftslagen. Genom att det krävs en särskild författning för att avvika från det integritetsskydd som personuppgiftslagen ger, ansågs det finnas en garanti för att behovet av särregler alltid övervägs noga i den ordning som gäller för författningsreglering.

8.2.2 Räcker personuppgiftslagens regler?

Bedömning: Personuppgiftslagens reglering är i sig inte tillräcklig för att täcka förpliktelseerna i rambeslutet.

Skälen för bedömningen

I de verksamheter och situationer där personuppgiftslagen är tillämplig finns det i och för sig regler som täcker de flesta förpliktelser som följer av rambeslutet, om än inte alla. Frågan är om det även i de fall där personuppgiftslagen är tillämplig kan behövas lagändringar.

Även om rambeslutet till stora delar bygger på dataskyddsdirektivet innehåller det delvis andra regler än detta. Skillnaderna beror på att rambeslutet har skraddarsyttts för utbyte över gränserna av information i brottsbekämpande verksamhet och annat straffrättsligt samarbete. Särskild hänsyn har tagits till det stora behovet av sekretess för att skydda den framtida verksamheten inom brottsbekämpningen. Det är t.ex. i större utsträckning än annars nödvändigt att undanhålla den registrerade information

om behandlingen, eftersom avslöjandet av att behandling pågår skulle kunna skada en brottsutredning eller hindra ett fungerande underrättelsearbete. Visserligen tar även regleringen i personuppgiftslagen hänsyn till sekretess, men i rambeslutet har de särskilda behoven av att kunna utbyta hemlig information om brott och brottslingar vägts in. Vidare har hänsyn tagits till att uppgifter av känsligt slag förekommer oftare i denna verksamhet än vid personuppgiftsbehandling i allmänhet och att det finns verksamhetsbehov av att kunna behandla sådana uppgifter. Även andra verksamhetshänsyn har vägts in, som exempelvis att informationen inte alltid kan vara verifierad och att uppgifter i juridiskt bindande beslut inte kan ändras även om vissa uppgifter i dessa har visat sig vara felaktiga.

Allmänt sett kan konstateras att den behandling som förekommer hos de brottsbekämpande myndigheterna, vid domstol och vid straffverkställighet ofta skiljer sig från den behandling som är tillåten enligt huvudreglerna i personuppgiftslagen. Detta är också huvudskälet till den omfattande särregleringen, som bör behållas. Åtskilligt av den behandling som är nödvändig för att de brottsbekämpande myndigheterna ska kunna utföra sin verksamhet skulle över huvud taget inte vara tillåten om inte undantag gjorts från vissa bestämmelser i personuppgiftslagen, exempelvis behandlingen av känsliga uppgifter. Det finns också ett påtagligt behov av avvikande eller mera preciserade regler för dessa verksamhetsområden än de allmänt hållna bestämmelserna i personuppgiftslagen. Avvikande regler kan behövas för att möjliggöra viss typ av behandling och mer preciserade regler utgör en viktig del av integritetsskyddet, t.ex. regler som begränsar åtkomst eller utlämnande. En särreglering kan således behövas både av verksamhetsskäl och för att skapa ett bättre integritetsskydd för vissa uppgifter.

Det sagda innebär att, även om det redan finns regler i personuppgiftslagen som helt eller delvis täcker de förpliktelser som följer av rambeslutet, det ändå kan vara nödvändigt eller lämpligt med särregler i de författningar som reglerar en viss sektor eller ett visst register. I de delar där rambeslutet innehåller andra eller

mera långtgående förpliktelser än dataskyddsdirektivet krävs naturligtvis också lagstiftning. Det finns emellertid anledning att utgå från den nuvarande regleringen i personuppgiftslagen på varje punkt där en särreglering diskuteras.

8.3 Rambeslutets syfte och tillämpningsområde

Bedömning: De inledande bestämmelserna kräver ingen lagstiftning.

Skälen för bedömningen

Allmänt om tillämpningsområdet

Syftet med rambeslutet är enligt *artikel 1* punkten 1 att säkerställa en hög skyddsnivå för fysiska personer när det gäller behandling av personuppgifter. Samma grundläggande syfte gäller för den svenska lagstiftningen som rör personuppgiftsbehandling, även om detta inte uttryckligen framgår av alla aktuella författningar. Det krävs dock inte någon komplettering av lagstiftningen i detta hänseende, eftersom punkten närmast kan ses som en programförklaring.

Rambeslutet är tillämpligt på behandling av personuppgifter inom ramen för polissamarbete och straffrättsligt samarbete enligt avdelning VI i fördraget om Europeiska unionen, dock enligt punkten 2 endast när personuppgifter samlas in, bearbetas eller behandlas på annat sätt i syfte att förebygga, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder. Detta innebär att polisiärt eller rättsligt samarbete i annat syfte faller utanför tillämpningsområdet. Rättslig hjälp i civilmål faller också utanför, liksom t.ex. informationsutbyte som rör offer för olyckshändelser även om informationen förmedlas via polisiära kanaler.

Tillämpningsområdet omfattar vidare enligt punkten 3 bara behandling av personuppgifter som utförs helt eller delvis automatiserat samt annan behandling av personuppgifter som ingår i eller är avsedda att ingå i register. Tillämpningsområdet motsvarar i denna del dataskyddsdirektivet, som varit utgångspunkten när man utformat särlagstiftningen. Författningarna om personuppgiftsbehandling inom polisen, Tullverket, Kustbevakningen, Skatteverket, åklagarväsendet, domstolsväsendet och kriminalvården har alla samma grundläggande tillämpningsområde som personuppgiftslagen och uppfyller därigenom kraven i rambeslutet. Vidare är dessa författningar inriktade på sådan verksamhet som anges i punkten 2. Några förändringar i fråga om tillämpningsområdet för de olika sektorsförfattningarna krävs därför inte.

De särskilda författningarna om enskilda register, exempelvis författningarna om belastningsregister, misstankeregister, straffförelägganderegister och ordningsbotsregister, reglerar behandlingen i ett eller flera register och faller därmed automatiskt under rambeslutets tillämpningsområde, eftersom registren i fråga har brottsbekämpning, lagföring eller straffverkställighet som ändamål. Som framgått ovan för polisen olika register som faller utanför tillämpningsområdet, exempelvis det centrala passregistret. Även Tullverket, Skatteverket och Kustbevakningen för register som ligger utanför tillämpningsområdet. Detsamma gäller vissa register som förs inom domstolsväsendet. Sådana register behandlas inte i det följande.

Undantag från tillämpningsområdet

I artikel 1 görs vissa undantag från tillämpningsområdet. Ett viktigt undantag är enligt punkten 4 nationella säkerhetsintressen och särskild underrättelseverksamhet som rör nationell säkerhet. Undantaget gäller alltså inte för den organisation som sysslar med frågor rörande nationell säkerhet utan för verksamheten som sådan. Så som undantaget är utformat faller det mesta av

Säkerhetspolisens verksamhet utanför tillämpningsområdet. I den utsträckning som Säkerhetspolisen har uppgifter som inte tar direkt sikte på nationell säkerhet omfattas myndigheten dock av rambeslutets tillämpningsområde. Ett exempel på detta är när Säkerhetspolisen biträder den övriga polisen eller Tullverket med hanteringen av hemliga tvångsmedel i deras verksamhet.

För närvarande regleras Säkerhetspolisens personuppgiftsbehandling på i huvudsak samma sätt som för polisen i övrigt. Polisdatalagen innehåller dock särskilda bestämmelser om Säkerhetspolisens register. I förslaget till lag om polisens behandling av personuppgifter i den brottsbekämpande verksamheten föreslås också särskilda regler för Säkerhetspolisens verksamhet. Flertalet av de ändamål som anges för Säkerhetspolisens personuppgiftsbehandling i det förslaget får anses inrymmas under begreppet nationell säkerhet, medan det är osäkert om så är fallet när det gäller andra. Som nyss nämnts faller Säkerhetspolisens biträde till andra myndigheter med hantering av tvångsmedel utanför. Personskydd för den centrala statsledningen torde kunna räknas som en form av skydd för nationell säkerhet, men knappast personskydd för andra kategorier. Delar av Säkerhetspolisens verksamhet kommer därmed sannolikt att beröras av rambeslutet. Eftersom Säkerhetspolisens personuppgiftsbehandling endast till mindre del avviker från vad som gäller för den övriga polisen, innebär det att regleringen i samma utsträckning antingen uppfyller kraven eller behöver förändras. Det finns därför inte skäl att i fortsättningen beröra Säkerhetspolisen särskilt.

Den viktigaste inskränkningen när det gäller tillämpningsområdet är att detta enligt artikel 1 punkten 2 enbart omfattar uppgifter som förs över eller görs tillgängliga, eller har överförts eller gjorts tillgängliga, mellan medlemsstater eller från medlemsstater till tredje land eller till internationella organisationer som sysslar med brottsbekämpning. Detta sätt att formulera tillämpningsområdet kan ge uppfattningen att tillämpningsområdet är mycket snävt.

Under förhandlingsarbetet har ett flertal stater, bland dem Sverige, motsatt sig att rambeslutet ska tillämpas på all nationell lagstiftning som rör personuppgiftsbehandling inom rambeslutets tillämpningsområde. Huvudskälen för detta var dels att rambeslutet i så fall skulle gå utöver Europeiska unionens rätt att besluta i mellanstatliga frågor, dels att det skulle kunna leda till kompromisser som för enskilda stater skulle innebära ett svagare integritetsskydd för den enskilde.

Under förhandlingarna har diskuterats om rambeslutet också bör omfatta alla uppgifter som *kan komma att* överföras eller göras tillgängliga mellan medlemsstater eller mellan medlemsstater och tredje land eller internationella organ. Den politiska överenskommelse som träffats om innehållet ställer inte krav på detta. Däremot är det en klart uttalad målsättning med rambeslutet att dataskyddet vid nationell behandling ska hålla samma standard som krävs enligt detta, i syfte att underlätta informationsutbytet inom Europeiska unionen (skäl 6 a).

Även om tillämpningsområdet formellt endast omfattar uppgifter som överförs eller görs tillgängliga, eller har överförts eller gjorts tillgängliga, innebär detta således inte att rambeslutet kan fränkännas betydelse för den nationella lagstiftningen och tillämpningen. Utgångspunkten bör därför vara att svensk lagstiftning anpassas till rambeslutet där detta är möjligt och lämpligt.

En annan begränsning ligger, som nyss nämnts, i att rambeslutet endast ska tillämpas på uppgifter som myndigheten har samlat in eller behandlar för att förebygga, utreda, upptäcka eller lagföra brott eller verkställa straffrättsliga påföljder. Det innebär t.ex. att uppgifter i vapenregister inte omfattas av tillämpningsområdet, eftersom uppgifterna i registret samlats in och behandlas för annat ändamål. Om sådana uppgifter förekommer i en förundersökning omfattas de dock av tillämpningsområdet, eftersom de då behandlas för ett annat ändamål.

Uppgifter som en medlemsstat har fått från en annan medlemsstat, men som har sitt ursprung i den första staten, omfattas inte heller av tillämpningsområdet (skäl 6 b). Undantaget ska ses

mot bakgrund av att överföring av uppgifter formellt inte påverkar den nationella lagstiftningen.

Rambeslutet är enbart tillämpligt på uppgifter som rör fysiska personer, medan den svenska lagstiftningen i viss utsträckning ger motsvarande skydd för juridiska personer, se exempelvis 19 § lagen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet. Detta utgör dock inte något problem, eftersom medlemsstaterna får ha regler som skapar ett starkare skydd nationellt (artikel 1 punkten 5 och skäl 6 a). Överföring av uppgifter om juridiska personer faller således utanför rambeslutet.

All personuppgiftsbehandling inom respektive verksamhetsområde som enbart är av administrativ natur, exempelvis behandling av personuppgifter som rör den egna personalen, faller också utanför tillämpningsområdet. Detta överensstämmer väl med den svenska lagstiftningen, där sådan personuppgiftsbehandling i sin helhet regleras genom personuppgiftslagen även för de brottsbekämpande myndigheterna, domstolsväsendet och Kriminalvården.

Sammanfattningsvis torde rambeslutets bestämmelser om tillämpningsområdet i sig inte kräva några lagändringar.

Definitioner

Artikel 2 i rambeslutet innehåller vissa definitioner. Dessa är i allt väsentligt desamma som i dataskyddsdirektivet. De motsvarar således de definitioner som finns i 3 § personuppgiftslagen, som gäller för den lagstiftning som berörs av rambeslutet.

Det finns även definitioner av begreppen ”behöriga myndigheter” och ”avidentifiering”. Med behöriga myndigheter avses dels myndigheter som inrättats genom rådsakter enligt avdelning VI i fördraget om Europeiska unionen, dels polis, tull, domstolar eller andra behöriga myndigheter i medlemsstaterna som genom nationell lagstiftning är bemyndigade att behandla personuppgifter inom tillämpningsområdet för rambeslutet. Med avidentifiering avses att ändra personuppgifter på sådant sätt att detal-

jerna beträffande personliga eller sakliga förhållanden inte längre eller endast med oproportionerlig stor insats i fråga om tid, kostnader och arbete kan tillskrivas en identifierad eller identifierbar fysisk person.

Dessa definitioner är inte av den arten att de måste införas i svensk lagstiftning.

8.4 Ändamålen med behandlingen

Bedömning: De flesta författningar som berörs uppfyller kraven på tydliga och berättigade ändamål. Däremot kan det behövas kompletterande regler som begränsar möjligheten till vidarebehandling av uppgifter som har överförts eller gjorts tillgängliga av en annan stat.

Innehållet i rambeslutet

Enligt *artikel 3* får personuppgifter endast samlas in för särskilda, uttryckligt angivna och berättigade ändamål och uppgifterna får endast behandlas för det ändamål som låg till grund för insamlingen av dem. Behandlingen måste vidare vara befogad, adekvat och relevant. Vidarebehandling för annat ändamål är tillåten om tre förutsättningar är uppfyllda. För det första ska behandlingen inte vara oförenlig med det ändamål för vilket uppgifterna samlades in. I skäl 5 a framhålls att det får avgöras på nationell nivå vilka ändamål som ska anses vara oförenliga med det ändamål för vilket personuppgifterna ursprungligen insamlades. För det andra ska den behandlande myndigheten vara behörig att utföra behandlingen. För det tredje ska behandlingen vara nödvändig och stå i proportion till ändamålet.

Personuppgifter får dessutom alltid behandlas vidare för historiska, statistiska eller vetenskapliga ändamål, under förut-

sättning att medlemsstaterna föreskriver lämpliga skyddsåtgärder, såsom avidentifiering av uppgifterna.

Flera artiklar innehåller begränsningar för hur överförda uppgifter får vidarebehandlas. Enligt *artikel 12* får personuppgifter, som översänts eller gjorts tillgängliga av en medlemsstat vidarebehandlas, i enlighet med kraven i artikel 3.2, för andra ändamål än de för vilka de översändes eller gjordes tillgängliga *endast*

- för att förebygga, utreda, upptäcka eller lagföra andra brott eller för att verkställa andra straffrättsliga påföljder,
- för andra rättsliga eller administrativa förfaranden med direkt anknytning till sådan verksamhet,
- för att avvärja en överhängande och allvarlig fara för den allmänna säkerheten, eller
- för varje annat ändamål, om den översändande staten eller den registrerade har samtyckt till det enligt sin nationella lagstiftning.

Uppgifterna får dessutom behandlas vidare för historiska, statistiska eller vetenskapliga ändamål under samma förutsättningar som anges i artikel 3.

På begäran av den myndighet som har översänt uppgifter eller gjort dem tillgängliga ska, enligt *artikel 15*, mottagaren ge besked om hur uppgifterna behandlas.

Personuppgiftslagen

Artiklarna 3 och 12 motsvarar delvis artikel 6 punkten 1 i data-skyddsdirektivet, som återspeglas i 9 § personuppgiftslagen. Den paragrafen innehåller bl.a. en regel om att personuppgifter endast får samlas in för särskilda, uttryckligt angivna och berättigade ändamål. Vidare föreskrivs att personuppgifter inte får vidarebehandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in (den s.k. finalitetsprincipen). Uppgifterna ska också vara adekvata och relevanta i förhållande till

ändamålen med behandlingen (första stycket punkterna c, d och e).

Personuppgifter får enligt 9 § första stycket punkten i inte bevaras under längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen. Enligt 9 § andra stycket får dock personuppgifter bevaras för historiska, statistiska eller vetenskapliga ändamål under längre tid. Möjligheten att använda personuppgifter som bevaras för sådana ändamål är dock begränsad. De får användas för att vidta åtgärder mot den registrerade bara om denne har samtyckt till det eller om det finns synnerliga skäl med hänsyn till den registrerades vitala intressen. Undantag görs också för myndighets användning av uppgifter i allmänna handlingar (8 § andra stycket personuppgiftslagen)

Personuppgiftslagens regler om grundläggande krav på behandlingen torde gälla inom de nu aktuella verksamhetsområdena, om det inte finns avvikande regler. För Tullverkets del finns en direkt hänvisning till vissa delar av 9 § personuppgiftslagen. Där görs dock undantag för personuppgiftslagens regel om vidarebehandling.

Skälen för bedömningen

Ändamålen för den grundläggande behandlingen

Integritetsskyddskommittén har i sitt slutbetänkande framhållit att ett av de från integritetsskyddssynpunkt viktigaste momenten i hanteringen av personuppgifter handlar om ändamålet med behandlingen. Det finns därför skäl att fokusera på den frågan när det gäller genomförandet av rambeslutet.

De författningar som reglerar enskilda register har klara och tydliga ändamål angivna. Detsamma gäller de flesta av de sektorsförfattningar som berörs av rambeslutet. Det ligger dock i sakens natur att ändamålen för ett verksamhetsområde dels måste formuleras tämligen generellt, dels i viss utsträckning kan komma att överlappa varandra. I ett fall, nämligen förordningen

om åklagarväsendets personuppgiftsbehandling, kan det ifrågasättas om ändamålet inte kan uttryckas tydligare. Den aktuella författningen är emellertid föremål för översyn (se avsnitt 6.8.). Man kan utgå från att frågan om ändamålet behöver preciseras då kommer att övervägas. Kravet på klara och tydliga ändamål för insamling och behandling är således uppfyllt beträffande de flesta författningarna men måste naturligtvis beaktas i det fortsatta arbetet, eftersom så många av författningarna är föremål för översyn.

Vidarebehandling för historiska, statistiska eller vetenskapliga ändamål

Däremot innehåller författningarna som regel inte några bestämmelser om tillåtna ändamål för vidarebehandling, utöver behandling för historiska, statistiska eller vetenskapliga ändamål. Sådan behandling är, som framgått ovan, tillåten men bara under förutsättning att medlemsstaterna föreskriver lämpliga skyddsåtgärder. Motsvarande krav ställs i dataskyddsdirektivet (artikel 6 punkten 1 b). I propositionen om personuppgiftslag diskuterades ingående huruvida den svenska arkivlagstiftningen uppfyllde kraven i direktivet. Regeringen ansåg att så var fallet (prop. 1997/98:44 s. 47 f.) och riksdagen anslöt sig till detta.

De flesta av sektorsförfattningarna innehåller en reglering som motsvarar personuppgiftslagens i fråga om vidarebehandling för nu aktuella ändamål. Det finns dock några undantag. Tullverkets författning lämnar utrymme för att handlingar bevaras i stället för att gallras, men anger inte för vilka ändamål dessa får bevaras. Den bestämmelsen kan därför behöva ses över. Domstolsväsendets författningar utgår från att uppgifterna gallras från datamediet men överförs till pappersform. Frågan om vidarebehandling för historiska, statistiska eller vetenskapliga ändamål saknar därför, med dagens reglering, betydelse för domstolarnas del.

Rambeslutet torde således, med något enstaka undantag, inte kräva några lagändringar när det gäller vidarebehandling för historiska, statistiska eller vetenskapliga ändamål.

Förhållandet till offentlighetsprincipen

Offentlighetsprincipen enligt 2 kap. tryckfrihetsförordningen innebär att myndigheterna är skyldiga att – i den utsträckning sekretess inte hindrar det – lämna ut allmänna handlingar till den som begär det. Eftersom utlämnande utgör en form av behandling har Sverige begärt, och fått, ett undantag i form av en förklaring i skäl 15 a att rambeslutet tillåter att principen om handlingars offentlighet tas med i bedömningen vid genomförandet av rambeslutet. Behandling som sker för att uppfylla kraven i den svenska offentlighetsprincipen kan således inte ses som oförenlig med de ändamål för vilka uppgifterna har samlats in.

Vilken annan vidarebehandling är tillåten?

Rambeslutet tillåter alltid vidarebehandling för de ändamål som har störst praktisk betydelse från verksamhetssynpunkt, nämligen för att förebygga, upptäcka, utreda eller lagföra andra brott än de som föranledde att uppgifterna sändes över eller gjordes tillgängliga samt för verkställighet av annan påföljd (artikel 12 punkten 1 a). Däremot kan kravet i artikel 10 punkten 1 på att den andra statens gallringsfrister ska iakttas innebära ett hinder mot vidarebehandling i enstaka fall, nämligen om vidarebehandlingen aktualiseras först en tid efter överföringen eller om den andra staten har särskilt korta gallringsfrister. Vid pågående utredningsarbete, lagföring eller verkställighet får dock uppgifterna bevaras för att fullfölja den uppgiften, även om den andra statens gallringsfrist har löpt ut.

Det är också tillåtet att vidarebehandla uppgifter för andra administrativa och rättsliga förfaranden som är direkt knutna till

förebyggandet, upptäckandet, utredningen eller lagföringen av brott eller till verkställigheten (artikel 12 punkten 1 b). Det torde innebära att uppgifterna exempelvis får användas för indrivningen av skadestånd, företagsbot eller andra ekonomiska åligganden i en brottmålsdom. Vidare bör de kunna användas exempelvis i nådeärenden eller i ärenden som rör ändring av påföljd. Särskild förverkandetalan angående utbyte av brottslig verksamhet kan vara ett annat exempel. Likaså bör de kunna vidarebehandlas för att ta ut skatt, tull eller andra avgifter som är direkt relaterade till det brott för vilket de översändes. Däremot torde det inte vara tillåtet – utan samtycke av den översändande staten – att använda uppgifter som en svensk myndighet har fått från en annan stat i samband med brottsutredning som grund för t.ex. en allmän upptaxering eller för att klarlägga en persons ekonomiska villkor för indrivning av andra skulder än sådana som är kopplade direkt till brottet, eftersom sådan behandling inte kan sägas ha en direkt anknytning till de primära ändamålen.

När det gäller möjligheten att vidarebehandla uppgifter som har översänts från en annan stat för att avvärja en överhängande och allvarlig fara för allmän säkerhet torde utrymmet inte vara särskilt stort. Kravet i artikel 12 punkten 1 c bör tolkas så att vidarebehandling är tillåten framför allt i de fall där man inte hinner kontakta den andra staten därför att behovet av att agera har uppkommit plötsligt. Dessutom bör kravet på att faran ska vara allvarlig ses som ett mått på att det måste finnas ett tydligt samhällsintresse att avvärja denna, som t.ex. när organiserade bedrägerier riktar sig mot finanssystemet. Man kan även tänka sig situationer där polisen behöver gå ut med en varning till allmänheten på grund av att man upptäckt systematiska brott som kan vålla stor skada för samhället. Omfattande spridning av datavirus eller manipulation av större datasystem kan vara exempel på det, liksom omfattande spridning av falska sedlar eller andra betalningsmedel.

Det kan också finnas skäl att erinra om att vidarebehandling för detta ändamål kan överlappas av vidarebehandling för utredning eller lagföring av brott. Eftersom man i svensk lagstiftning,

i större utsträckning än i många andra länder, straffbelägger gärningar på förberedelse- och försöksstadiet samt har vidsträckta jurisdiktionsregler kan uppgifter om ett brott som riktar sig mot Sverige eller svenska intressen inte sällan utredas och lagföras i Sverige.

Generellt sett finns det dock anledning att iaktta viss försiktighet när det gäller tolkningen av utrymmet för vidarebehandling. Det torde vara bättre att vid tveksamhet vända sig till den berörda staten och försöka utverka medgivande till vidarebehandling i det konkreta fallet än att tolka in för mycket i de generella reglerna i rambeslutet. Vidarebehandling får nämligen ske för vilket annat ändamål som helst, under förutsättning att den översändande staten har lämnat medgivande till det i enlighet med sin nationella lagstiftning (se artikel 12 punkten 1 d).

Det bör noteras att ett medgivande till vidarebehandling av uppgifter som har översänts från en annan stat, beroende på den enskilda statens nationella lagstiftning, kan lämnas i form av ett allmänt samtycke till vidarebehandling av kategorier av information eller för viss typ av behandling (se skäl 11 a). Det sagda innebär att det inte finns något som hindrar att en stat som översänder uppgifter redan vid översändandet förklarar att viss vidarebehandling, utöver vad som anges i artikel 12, är tillåten eller att den mottagande staten får förfoga fritt över informationen. Det kan finnas anledning att i det fortsatta arbetet överväga nyttan av att lämna sådant samtycke i de fall där det är förenligt med svenska intressen att uppgifterna får användas för andra ändamål än de ursprungliga. I den mån det bör regleras torde det kunna ske i förordning.

Om vidarebehandling är tillåten, ska reglerna i artikel 3 punkten 2 tillämpas. Det innebär att behandlingen för det nya ändamålet ska utföras av en behörig myndighet, vara nödvändig och stå i proportion till ändamålet. Uppgifterna får inte heller behandlas under längre tid än vad som krävs för det nya ändamålet.

Behövs det särskilda regler för vidarebehandling?

Rambeslutet ställer, som framgått ovan, mer preciserade krav än dataskyddsdirektivet när det gäller annan vidarebehandling än för historiska, statistiska eller vetenskapliga ändamål. Eftersom rambeslutet förpliktar medlemsstaterna att införa lagstiftning som hindrar vidarebehandling för andra ändamål än de som anges i artikel 12 krävs det således författningsreglering. Begränsningarna i fråga om vidarebehandling har i huvudsak intresse för situationer där den mottagande myndigheten själv vill vidarebehandla uppgifter för ett helt annat ändamål än brottsbekämpning eller vill lämna uppgifterna vidare till en myndighet som varken sysslar med brottsbekämpning, lagföring eller verkställighet av straff. Begränsningarna är därför trots allt inte så stora.

När det gäller den framtida behandlingen av personuppgifter i polisens brottsbekämpande verksamhet har föreslagits att 9 § personuppgiftslagen ska gälla i vissa delar, men att undantag ska göras från finalitetsprincipen (Ds 2007:43 s. 112 ff.). I stället anges uttömmande i lagen för vilka ändamål behandling får ske. Dessa ändamål är i stort väl förenliga med artikel 12, men innehåller inte några inskränkningar beträffande information som erhållits från andra stater. Det torde därför bli nödvändigt att införa bestämmelser om detta. Däremot föreslås att finalitetsprincipen ska gälla för den framtida personuppgiftsbehandlingen inom Kustbevakningen (SOU 2006:18 s. 97). Som framgått ovan ger dock inte heller den uttryck för de inskränkningar som krävs när det gäller vidarebehandling av uppgifter som översänts av en annan stat. För Tullverkets del har man valt samma teknik som för polisen, dvs. det anges uttömmande för vilka ändamål behandling får ske. Den lagen torde således också behöva kompletteras, av samma skäl som angetts för polisens del. Detsamma gäller för åklagarväsendets, Skatteverkets och kriminalvårdens författningar.

Däremot torde det inte krävas några lagstiftningsåtgärder för domstolarnas del, eftersom frågan om vidarebehandling knappast aktualiseras där.

När det gäller de särskilda registerförfattningarna, exempelvis lagarna om belastningsregister och misstankeregister, torde det inte heller krävas några lagstiftningsåtgärder, eftersom den behandling som äger rum där kan sägas vara en produkt av vidarebehandlingen hos någon av de brottsbekämpande myndigheterna. En uppgift som inte får vidarebehandlas hos en brottsbekämpande eller verkställande myndighet bör därför aldrig nå registren. Härtill kommer att, även om så skulle vara fallet, den behandling som sker i de särskilt reglerade registren alltid sker för ändamål som är tillåtna enligt artikel 12.

Behandling av kvarstående misstankar

Flera sektorsförfattningar innehåller bestämmelser om behandling av kvarstående misstankar, vilket möjligen kan betraktas som en form av vidarebehandling. Sådan behandling, som alltid görs i brottsbekämpande syfte, kan inte anses oförenlig med det ursprungliga ändamålet och kravet på att myndigheten som utför behandlingen är behörig utgör inte heller något problem. De krav som ställs upp för förnyad behandling får också anses uppfylla kraven på att behandlingen ska vara nödvändig och proportionerlig. Bestämmelserna om behandling av kvarstående misstankar torde därför inte behöva ändras av hänsyn till rambeslutet. Frågan om sådana regler är förenliga med kravet på gallring finns det skäl att återkomma till.

Behandling av uppgifter från avslutade brottsutredningar

I detta sammanhang finns det anledning att nämna ett av förslagen rörande polisens framtida personuppgiftsbehandling. Enligt förslaget till 3 kap. 12 § lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet får uppgifter i en förundersökning, som lett till åtal eller annan domstolsprövning, behandlas i polisens brottsbekämpande verksamhet upp till fem

år efter domen eller beslutet. Motsvarande ska gälla för uppgifter i en nedlagd förundersökning eller annan motsvarande utredning, men då räknas femårsfristen från åklagarens eller förundersökningsledarens beslut. Om denne i samband med beslutet har angett att brottet, trots beslutet, kan komma att bli föremål för lagföring får behandling ske fram till dess att brottet preskriberas. Syftet med förslaget är att tillgodose polisens behov av uppgifter bl.a. för att kunna utreda nya brott av eller mot samma person eller för att samla information om vissa typer av brott eller vissa brottslingars beteenden (se Ds 2007:43 s. 273 ff.).

Det råder inte någon tvekan om att rambeslutet medger att uppgifter som härrör från avslutade brottsutredningar i vissa fall vidarebehandlas, även om huvudregeln är att uppgifterna ska gallras när det inte längre finns något behov av dessa för det ursprungliga ändamålet. Vidarebehandling som sker i syfte att förebygga, upptäcka, utreda eller lagföra ett annat brott är alltid tillåten. Det råder således ingen tvekan om att vidarebehandling kan ske om uppgifterna behövs för att handlägga konkreta brottsmisstankar. Likaså måste de få användas t.ex. för att berika pågående underrättelsearbete eller för att verkställa en existerande påföljd. Det kan också vara nödvändigt för polisen att bevara och behandla information om brott och brottstyper för specifika ändamål, t.ex. att jämföra tillvägagångssättet vid allvarliga brott eller att övervaka seriebrottslingar. Frågan är emellertid om det kan anses vara förenligt med kraven i rambeslutet på proportionalitet och nödvändighet att, utan en bedömning i det enskilda fallet av intresset av uppgifterna, tillåta behandling av *all* information i *samtliga* brottsutredningar i fem år efter det att saken avslutades och oberoende av om det skedde genom en fällande dom eller genom annat beslut. Den frågan får bedömas i det fortsatta arbetet.

Information på begäran av översändande myndighet

Bestämmelsen i artikel 15, som enbart innehåller en skyldighet att på begäran ge den översändande myndigheten besked om hur uppgifterna behandlas, bör kunna genomföras i förordningsform.

Sammanfattande bedömning

Begränsningarna i fråga om annan vidarebehandling än för historiska, statistiska eller vetenskapliga ändamål torde alltså kräva vissa lagändringar om Sverige till alla delar ska uppfylla rambeslutets krav. Nya regler om begränsningar av möjligheterna till vidarebehandling behöver dock bara gälla för uppgifter som har överförts från en annan medlemsstat till en svensk myndighet eller som har gjorts tillgängliga för en svensk myndighet av en annan stat. Som utvecklas närmare i avsnitt 8.7 torde en sådan reglering förutsätta någon form av märkning av information som härrör från en annan stat.

8.5 Behandling av känsliga personuppgifter

Bedömning: Det finns redan regler om behandling av känsliga personuppgifter inom de verksamheter som berörs av rambeslutet. Vissa regler kan dock behöva ses över.

Skälen för bedömningen: I *artikel 7* i rambeslutet regleras behandling av vad som brukar kallas känsliga personuppgifter. Med detta avses personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening samt uppgifter som rör hälsa eller sexualliv. Enligt artikeln får sådana uppgifter behandlas endast när det är absolut nödvändigt och om det föreskrivs adekvata

skyddsåtgärder i den nationella lagstiftningen. Rambeslutets bestämmelser om behandling av känsliga personuppgifter skiljer sig således från de i dataskyddsdirektivet, där det ställs upp andra typer av begränsningar för behandling. Dessa återspeglas i 13–19 §§ personuppgiftslagen.

De författningar som innehåller särregler för personuppgiftsbehandlingen hos polisen, åklagare, Tullverket, Kustbevakningen, Skatteverket, domstolarna och kriminalvården innehåller samtliga i större eller mindre utsträckning bestämmelser om behandling av känsliga uppgifter som avviker från personuppgiftslagens.

Däremot finns det inga sådana regler i de registerförfattningar som reglerar enskilda register. Detta ska ses mot bakgrund av att dessa normalt har preciserade bestämmelser om vilka typer av uppgifter som får finnas i registren och att bestämmelserna om innehållet i praktiken inte tillåter registrering av känsliga uppgifter. Mot den bakgrunden finns det inget behov av att reglera förekomsten av känsliga uppgifter i dessa författningar.

Särreglerna om behandling av känsliga uppgifter i sektorsförfattningarna tillåter visserligen behandling i större utsträckning än personuppgiftslagen, men har i de flesta fall utformats så att möjligheten att behandla känsliga uppgifter är mycket begränsad. Många av bestämmelserna fordrar att behandlingen ska vara absolut nödvändig, vilket står i god överensstämmelse med innehållet i rambeslutet. Reglerna innehåller dessutom andra preciseringar, t.ex. i form av förbud att använda känsliga uppgifter som sökbegrepp. De regler som gäller för flertalet verksamhetsområden kan därmed anses uppfylla kraven i rambeslutet. Detsamma gäller förslagen till ny lagstiftning för polisen och Kustbevakningen.

Enligt de författningar som reglerar domstolsväsendets personuppgiftsbehandling är behandling av känsliga uppgifter tillåten i två olika situationer; dels om uppgifterna har lämnats i ett mål eller ärende dels om de behövs för handläggningen av målet eller ärendet. Någon föreskrift om att behandlingen ska vara

absolut nödvändig, vilket rambeslutet kräver, finns inte i dessa författningar. Att tillåta behandling av en inkommen handling torde ändå vara förenligt med kravet på att behandlingen är absolut nödvändig, så som den svenska lagstiftningen reglerar hanteringen av allmänna handlingar. Däremot kan det behövas mer begränsande regler för annan behandling. En föreskrift om att känsliga personuppgifter får behandlas därför att de "behövs för handläggningen" torde inte ensamt uppfylla kraven i rambeslutet på att behandlingen ska vara absolut nödvändig och att det ska finnas adekvata skyddsåtgärder.

8.6 Korrigerig av personuppgifter

Bedömning: De befintliga reglerna om rättelse uppfyller kraven i rambeslutet. Däremot torde de författningar som saknar regler om rättelse behöva ändras. Vissa författningsändringar torde alltså krävas.

Innehållet i rambeslutet

Artikel 4 innehåller regler om rättelse, radering och blockering. Syftet med artikeln är att tillgodose kvaliteten på uppgifterna. Bestämmelser om gallring, dvs. om radering eller utplånande av andra skäl än att uppgifterna inte håller tillräcklig kvalitet, finns i artikel 6. Den frågan behandlas i avsnitt 8.9.

Den grundläggande principen, som slås fast i artikel 4 punkten 1, är att personuppgifter ska rättas om de är felaktiga samt, om så är möjligt och nödvändigt, kompletteras eller aktualiseras. Om det finns skäl att anta att en radering av personuppgifter skulle påverka den registrerades intressen ska uppgifterna blockeras i stället. Blockerade uppgifter får endast behandlas för det ändamål som hindrade att de raderades.

Från kravet på radering görs i punkten 4 undantag för personuppgifter som ingår i ett domstolsbeslut eller underlaget för ett sådant beslut. I fråga om sådana uppgifter ska rättelse, radering eller blockering utföras enligt nationell lagstiftning. I skäl 8 a framhålls också att kravet på korrekthet måste ses på ett annat sätt när det gäller uppgifter i rättsliga förfaranden. Uppgifterna grundar sig ofta på personers subjektiva uppfattningar och då hänför sig kravet på korrekthet inte till innehållet i utsagan utan till det faktum att en viss utsaga har avgetts.

I *artikel 9* föreskrivs att myndigheterna ska vidta alla rimliga åtgärder för att se till att personuppgifter som är felaktiga, ofullständiga eller inaktuella inte överförs eller görs tillgängliga. I görligaste mån ska kvaliteten på uppgifterna kontrolleras innan dessa överförs eller görs tillgängliga. Dessutom ska alltid så långt möjligt annan information bifogas som gör att den mottagande myndigheten kan bedöma om uppgifterna är korrekta, fullständiga, aktuella och tillförlitliga. Om personuppgifter översänds spontant ska den mottagande myndigheten utan dröjsmål bedöma om uppgifterna är nödvändiga för det ändamål för vilka de översändes.

Skulle det visa sig att felaktiga uppgifter har översänts, eller att uppgifter har översänts olovligen, ska mottagaren enligt artikel 9 punkten 2 omedelbart underrättas om detta. Uppgifterna ska då omgående rättas, raderas eller blockeras i enlighet med artikel 4. Det innebär, som nyss nämnts, bl.a. att radering inte behöver ske i domstolsbeslut och underlaget för dem. När det gäller sådana uppgifter ska vidare, enligt skäl 8 d, rättelse, radering eller blockering ske enligt nationell rätt, om de behandlas av "kvasijudiciella myndigheter". Med detta avses myndigheter med behörighet att fatta rättsligen bindande beslut.

Enligt *artikel 18* punkten 1 ska medlemsstaterna fastställa om den registrerade har rätt att vända sig direkt till den personuppgiftsansvarige eller till tillsynsmyndigheten för att begära att den personuppgiftsansvarige fullgör sina uppgifter att rätta, radera eller blockera personuppgifter. Vägrar den personuppgiftsansvarige att rätta, radera eller blockera uppgiften, ska beslutet vara

skriftligt och innehålla uppgift om hur den berörde kan anföra klagomål eller på annat sätt begära prövning enligt nationell rätt. Den registrerade har rätt att få besked om huruvida behandlingen har varit korrekt eller inte. Medlemsstaterna får dock även föreskriva att den registrerade endast ska informeras av tillsynsmyndigheten om att en kontroll av behandlingen har utförts.

Om den registrerade bestrider att en viss uppgift är korrekt, och det inte kan fastställas om så är fallet, får uppgiften enligt punkten 2 märkas.

Personuppgiftslagen

Artiklarna 4 och 9 i rambeslutet motsvarar delvis artikel 6 d i dataskyddsdirektivet, som i sin tur återspeglas i 9 § personuppgiftslagen. Enligt första stycket punkterna g och h i den paragrafen föreskrivs att de uppgifter som behandlas ska vara riktiga och, om det är nödvändigt, aktuella samt att den personuppgiftsansvarige ska se till att alla rimliga åtgärder vidtas för att rätta, blockera eller utplåna sådana personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålen med behandlingen.

De nu aktuella punkterna i 9 § gäller vid Tullverkets personuppgiftsbehandling. De föreslås också gälla för polisens framtida personuppgiftsbehandling (Ds 2007:43 s. 112 f.), liksom för Kustbevakningens (SOU 2006:18 s. 196) och domstolarnas (SOU 2001:100 s. 108) och torde redan i dag vara tillämpliga där.

Artikel 18 motsvarar delvis artikel 12 b och c i dataskyddsdirektivet, som har genomförts genom regeln i 28 § personuppgiftslagen. Enligt den paragrafen är den personuppgiftsansvarige skyldig att på begäran av den registrerade snarast rätta, blockera eller utplåna personuppgifter som inte har behandlats korrekt enligt lagen eller föreskrifter som utfärdats med stöd av lagen.

En åtgärd av det nu aktuella slaget förutsätter dock att den personuppgiftsansvarige har övertygats om att uppgiften i fråga är felaktig (prop. 1997/98:44 s. 87). Om så inte är fallet kan den registrerade anmäla saken till tillsynsmyndigheten, som, om den

delar den registrerades uppfattning och inleder tillsyn, har möjlighet att försöka åstadkomma rättelse på frivillig väg eller förbjuda den personuppgiftsansvarige att behandla personuppgifterna på något annat sätt än genom att lagra dem. Som en sista utväg kan tillsynsmyndigheten föra talan vid domstol om att uppgifterna ska utplånas (47 § personuppgiftslagen).

Den registrerade kan också, om det rör sig om en myndighets behandling av personuppgifter, själv överklaga den personuppgiftsansvariga myndighetens beslut angående rättelse (52 § personuppgiftslagen).

Skälen för bedömningen

Behövs det lagändringar?

Rambeslutet innehåller olika förpliktelser när det gäller korrigering av personuppgifter, varav många överensstämmer med regleringen i dataskyddsdirektivet.

Från kravet på rättelse görs ett viktigt undantag i artikel 4 punkten 4 i rambeslutet som innebär att felaktiga uppgifter i domstolsbeslut och underlaget för dem inte behöver raderas. Undantaget täcker alla former av domstolsbeslut. Uppgifter som har flutit in i exempelvis en dom kan visserligen vara sakligt felaktiga, men dessa behöver ändå inte rättas. Undantaget ska ses mot bakgrund av att det skulle kunna leda till orimliga resultat om t.ex. de uppgifter som har lagts till grund för en frikännande dom, och som visar att vissa uppgifter som förebragts i rättegången är felaktiga, skulle medföra att de felaktiga uppgifterna måste tas bort från domen eller rättegångsmaterialet. Även åklagarbeslut som är rättsligen bindande omfattas av undantaget och detsamma torde gälla motsvarande beslut av annan, så som skäl 8 d får tolkas.

Någon motsvarande begränsning finns inte 9 § personuppgiftslagen. I det fortsatta arbetet bör därför övervägas behovet av att införa regler som speglar detta undantag.

När det gäller skyldigheten att på begäran av den registrerade rätta uppgifter är, genom hänvisningar i respektive sektorsförfattning, 28 § personuppgiftslagen tillämplig på personuppgiftsbehandlingen vid de myndigheter som berörs av rambeslutet.

I 12 § lagen om Schengens informationssystem finns en särskild rättelseregul. Där föreskrivs att Rikspolisstyrelsen är skyldig att på begäran av den registrerade, eller om det annars finns anledning till det, snarast rätta, blockera eller utplåna en personuppgift som styrelsen har registrerat, om uppgiften är rättsligt eller sakligt felaktig. Bestämmelsen torde uppfylla kraven i de nu aktuella artiklarna.

Förordningen om register över förelägganden av ordningsbot innehåller varken någon regel om rättelse eller någon hänvisning till personuppgiftslagens regel om rättelse. Så som personuppgiftslagens regel är utformad gäller den enbart rättelse av uppgifter som behandlats felaktigt med stöd av den lagen eller föreskrifter som har utfärdats med stöd av den. Den är således inte tillämplig på en särregling som saknar motsvarande bestämmelse. Däremot torde den kunna tillämpas på sådan felaktig behandling i registret som strider mot någon av personuppgiftslagens bestämmelser som är tillämplig på registret. Här krävs således en författningsändring för att uppfylla kraven i rambeslutet.

I 16 § förordningen om register över strafförelägganden föreskrivs att om en uppgift som har lämnats till belastningsregistret, misstankeregistret eller till Kronofogdemyndighetens utsökings- och indrivningsdatabas rättas, ska även den rättade uppgiften lämnas till registren. Den rättelse som åsyftas torde vara rättelse enligt 48 kap. 12 a § rättegångsbalken. Någon regel om att felaktiga personuppgifter ska rättas finns däremot inte. Regleringen har därför samma brist som regleringen av ordningsbotsregistret. Frågan torde komma att uppmärksammas vid den översyn som pågår (se avsnitt 6.8).

Övriga författningar om enskilda register innehåller samtliga hänvisningar till 28 § personuppgiftslagen som gör rättelseregeln tillämplig.

När det gäller radering måste också den svenska offentlighetsprincipen tas med i bedömningen. I de fall där någon har begärt att få del av en allmän handling får denna inte förstöras, även om det normalt hade kunnat ske. Vidare kan ändringar inte göras i allmänna handlingar enbart därför att någon kräver att en felaktig uppgift raderas. I förarbetena till personuppgiftslagen gjordes en ingående analys av förhållandet mellan dataskyddsdirektivet och den svenska reglering av tryck- och yttrandefrihet. För en närmare beskrivning av detta, se prop. 1997/98:44 s. 49 ff.

Enligt skäl 15 a medger rambeslutet att offentlighetsprincipen beaktas vid genomförandet. En förpliktelse som skulle komma att stå i strid med de grundläggande principerna i andra kapitlet tryckfrihetsförordningen behöver således inte genomföras i den svenska lagstiftningen.

Sammanfattande bedömning

De befintliga reglerna om rättelse av personuppgifter uppfyller kraven i rambeslutet. Detta inbegriper de författningar som hänvisar till 28 § personuppgiftslagen. I de fall där det inte finns någon regel om rättelse av personuppgifter måste en sådan införas eller en hänvisning göras till personuppgiftslagen.

Frågan om det i tillräcklig utsträckning finns regler om rätt att överklaga beslut om rättelse behandlas i avsnitt 8.12.

8.7 Överföring av uppgifter till tredje land eller till internationella organisationer

Bedömning: Det krävs lagstiftning som begränsar möjligheten att föra över uppgifter som erhållits från en annan medlemsstat till tredje land eller till internationella organisationer, utan föregående kontakt med den medlemsstat från vilken uppgiften härrör.

Innehållet i rambeslutet

Överföring av uppgifter till tredje land eller till internationella organ, eller organisationer som har inrättats genom internationella överenskommelser, regleras i *artikel 14*. Det uppställs stränga krav för att uppgifter, som erhållits från en annan medlemsstat, ska få föras över eller göras tillgängliga. Sådan överföring får ske endast om

- den är nödvändig för att förebygga, utreda, upptäcka eller lagföra brott eller för verkställighet av en straffrättslig påföljd,
- mottagaren har ansvar för sådan verksamhet,
- den stat från vilken uppgifterna har erhållits har gett samtycke till överföringen, samt
- mottagaren har en adekvat skyddsnivå för databehandling.

Samtliga dessa villkor måste således vara uppfyllda för att det ska vara tillåtet att föra över uppgifter eller att göra dessa tillgängliga för tredje land eller internationella organ.

Undantag från kraven på förhandsmedgivande till överföring medges endast om överföringen är absolut nödvändig antingen för att avvärja en omedelbar och allvarlig fara för allmän säkerhet eller för en medlemsstats väsentliga intressen och ett förhandsmedgivande inte hinner utverkas i tid. I sådana fall ska den myndighet som ska medge överföring underrättas utan dröjsmål.

Vissa undantag medges också från kravet på adekvat skyddsnivå hos mottagaren, nämligen om

- den nationella lagstiftningen hos den medlemsstat som överför uppgifterna föreskriver detta på grund av vissa viktiga intressen eller
- mottagaren sörjer för skyddsåtgärder som den översändande staten bedömer vara tillräckliga enligt sin lagstiftning.

Vid bedömningen av om skyddsnivån är adekvat ska hänsyn tas till alla relevanta omständigheter, bl.a. uppgifternas art, syftet med behandlingen och varaktigheten.

Personuppgiftslagen

Dataskyddsdirektivet föreskriver i artiklarna 25 och 26 begränsningar i möjligheterna att överföra uppgifter till tredje land som i stora delar överensstämmer med bestämmelserna i artikel 14 i rambeslutet. Det föreskrivs ett generellt förbud mot överföring av personuppgifter till tredje land i 33 § personuppgiftslagen, om landet inte har en adekvat nivå för skyddet av personuppgifterna. Vissa generella undantag från förbudet regleras i 34 §. De länder som har tillträtt Europarådets dataskyddskonvention (se avsnitt 4.2.3) anses enligt 34 § uppfylla kraven på en godtagbar skyddsnivå.

Särskilda regler om överföring av uppgifter till utländska myndigheter och organ

Som redovisats i avsnitt 4.7.7 innehåller flera av de författningar som nu är aktuella särskilda regler om utlämnande av uppgifter till utländska myndigheter och mellanfolkliga organisationer. Sådana regler finns i 7 § polisdatlagen och 17–18 §§ polisdataförordningen, 11 och 12 §§ lagen om belastningsregister, 9 och 10 §§ lagen om misstankeregister, 2 kap. 6 § lagen om internationellt tullsamarbete, 6 § lagen om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar och 18 § förordningen om behandling av personuppgifter inom åklagarväsendet.

Reglerna är i stort sett utformade på samma sätt. De tillåter att uppgifter lämnas om detta följer av en internationell överenskommelse som har godkänts av riksdagen. I något fall ställs inte krav på att det ska finnas ett godkännande av riksdagen utan det räcker med en för Sverige bindande överenskommelse som har träffats med en annan stat. Ett exempel på detta är 18 § förordningen om behandling av personuppgifter inom åklagarväsendet.

Skälen för bedömningen

Huvudsyftet med rambeslutet är att förbättra det gränsöverskridande informationsutbytet genom att tillförsäkra ett likvärdigt dataskydd. Rambeslutet har således samma fokus som dataskyddsdirektivet och personuppgiftslagen när det gäller överföring av uppgifter, men på ett område som inte regleras av dataskyddsdirektivet. Reglerna i artikel 14 om överföring av uppgifter till tredje land eller till internationella organisationer avviker i vissa avseenden från regleringen i personuppgiftslagen, även om det finns grundläggande likheter, t.ex. när det gäller hur man ska bedöma om det mottagande landet har en adekvat skyddsnivå.

Vissa sektorsförfattningar innehåller regler som tillkommit för att underlätta informationsutbytet med andra länder och med internationella organisationer som Interpol och Europol. Reglerna om uppgiftslämnande till annan stat eller till de nyss nämnda organisationerna innehåller inte några begränsningar av det slag som anges i artikel 14. I de lagar som reglerar internationellt samarbete för polisen, åklagarväsendet, Tullverket, Kustbevakningen, Skatteverket och kriminalvården kommer det därför att krävas nya bestämmelser om överföring till tredje land, eller internationella organisationer av sådana uppgifter som tidigare erhållits från en annan stat, som återspeglar dessa begränsningar. För domstolarnas del torde det för närvarande inte behövas några nya regler, eftersom dessa ytterst sällan har anledning att själva föra över uppgifter till andra stater eller till internationella organisationer (jfr SOU 2001:32 s. 129 ff.). Huruvida den framtida utvecklingen av det rättsliga samarbetet kan komma att leda till ett sådant behov är det för tidigt att ha någon uppfattning om.

Det bör dock betonas att rambeslutets begränsande regler endast omfattar sådana uppgifter som en svensk myndighet har fått från en annan medlemsstat eller som har gjorts tillgängliga av en annan medlemsstat. Även om det krävs lagändringar kan regleringen därför utformas så att den inte hämmar vare sig det in-

formationsutbyte som äger rum nationellt eller översändande av uppgifter som härrör från svenska myndigheter.

Det som framför allt krävs är någon form av märkning (eller ”flaggning”) av uppgifter som härrör från en annan medlemsstat, som gör den behandlande myndigheten uppmärksam på att uppgifterna inte får användas fritt. Varje överföring från en annan stat eller tillgängliggörande kommer nämligen att bära med sig användningsbegränsningar i fråga om överföring till tredje land eller till internationella organisationer – om inte den andra staten i samband med överförandet har gett sitt samtycke till fri användning. Om uppgifter som bär med sig en användarbegränsning inte är märkta finns det en uppenbar risk att någon annan än den som tog emot uppgifterna oavsiktligt använder dessa i strid med användningsbegränsningen. Det kan anmärkas att motsvarande hantering kommer att krävas för uppgifter som erhållits från en annan stat med stöd av Prümrådsbeslutet (se avsnitt 6.3).

8.8 Överföring av uppgifter till privata parter

Bedömning: Det krävs lagstiftning som begränsar möjligheten att föra över uppgifter som erhållits från en annan medlemsstat till privata parter.

Innehållet i rambeslutet

Artikel 14 a reglerar vidarebehandling i form av överföring av personuppgifter, som erhållits från en annan medlemsstat, till privata parter i medlemsstaterna. För sådan överföring ställs särskilt stränga krav. Överföring är tillåten endast om

- behörig myndighet i den andra staten har samtyckt till överföring och

- inga legitima intressen för den registrerade hindrar överföringen samt
- överföringen i det enskilda fallet är absolut nödvändig av något av de fyra följande skälen:
 1. för att utföra en författningssenlig uppgift
 2. för att förebygga, utreda, upptäcka eller lagföra brott eller verkställa straffrättsliga påföljder,
 3. för att avvärja en omedelbar och allvarlig fara för den allmänna säkerheten, eller
 4. för att hindra att enskildas rättigheter lider allvarlig skada.

Vid överföringen ska myndigheten underrätta mottagaren om för vilket ändamål uppgifterna uteslutande får användas.

Den nu aktuella regleringen berörs dock inte av att personuppgifter lämnas från domstolsväsendet, polisen eller tullväsendet till privata parter i brottmål, t.ex. till försvarsadvokater och brottsoffer (skäl 10 a).

Som exempel på när det kan vara nödvändigt att lämna uppgifter för att avvärja en omedelbar och allvarlig fara för allmän säkerhet och förhindra att enskilda personers rättigheter lider allvarlig skada nämns varningar till banker eller kreditinstitut om förfalskade värdepapper. Vidare nämns i fråga om fordonstölder uppgiftslämnande till försäkringsbolag för att hindra olaglig handel med stulna motorfordon och för att återföra stulna motorfordon från utlandet (skäl 10).

Det finns inte någon motsvarande regel i personuppgiftslagen.

Skälen för bedömningen

De stränga kraven i artikel 14 a för överföring av uppgifter som har överförts från eller gjorts tillgängliga av en annan stat har inte någon motsvarighet i svensk lagstiftning. Begränsningarna omfattar endast personuppgifter som har översänts från eller gjorts tillgängliga av en annan stat. Eftersom undantag från huvudprincipen har gjorts för sådan uppgiftslämnande som ut-

gör ett normalt led i brottmålsprocessen, nämligen uppgifter till parter i brottmål, dit även brottsoffer och försvarare räknas, torde begränsningarna inte bli så stora. De kräver dock ändringar i sektorsförfattningarna.

För domstolsväsendets del torde det inte krävas någon lagstiftning, med tanke på de undantag som nämns både i artikeln och i skäl 10 a. Det torde inte heller krävas några förändringar i de författningar som reglerar enskilda register.

Av samma skäl som angetts i avsnitt 8.7 kommer det att bli viktigt att i framtiden kunna märka personuppgifter som bär med sig begränsningar i fråga om möjligheten att överföra dem till privata parter.

8.9 Gallring

Bedömning: Den svenska lagstiftningen uppfyller i och för sig kraven i rambeslutet. Det kan dock finnas skäl att se över gallringsbestämmelserna i vissa författningar.

Innehållet i rambeslutet

Gallring regleras, som tidigare nämnts, i *artikel 6* i rambeslutet. Där föreskrivs att det ska fastställas lämpliga tidsfrister för radering av personuppgifter eller för omprövning av behovet att bevara uppgifterna. Medlemsstaterna ska införa förfaranderegler som garanterar att tidsfristerna efterlevs.

Enligt *artikel 4* punkten 2 ska personuppgifter, när de inte längre behövs för det ändamål för vilka de samlats in eller vidarebehandlats, raderas eller avidentifieras. Radering kan också ske genom att datamediet förstörs (skäl 8 c). Arkivering i en separat datamiljö i överensstämmelse med nationell rätt påverkas inte av regeln om radering i artikel 4. Sådan arkivering är dock tillåten endast om uppgifterna inte längre behövs i den brottsbekäm-

pande verksamheten eller för straffverkställighet. Arkiveringen behöver inte göras i en särskild databas, men däremot får uppgifterna inte längre användas för att förebygga, utreda, upptäcka eller lagföra brott eller för straffverkställighet (skäl 8 b).

När personuppgifter översänds till eller görs tillgängliga för en annan medlemsstat får, enligt *artikel 10*, den översändande staten underrätta mottagaren om de tidsfrister som gäller för gallring av uppgifterna. Mottagaren är då skyldig att, när fristen löper ut, radera eller blockera uppgifterna eller att göra en bedömning av om uppgifterna fortfarande behövs. Detta gäller dock inte om uppgifterna behövs för en pågående brottsutredning, lagföring eller verkställighet av påföljd, när fristen löper ut. Uppgifterna får då behållas för att fullfölja den uppgiften. Har den översändande myndigheten inte angett någon tidsfrist för gallring ska nationell rätt tillämpas.

Personuppgiftslagen

Artikel 6 punkten 1 e i dataskyddsdirektivet föreskriver att personuppgifter inte får bevaras under längre tid än som är nödvändigt för att de ändamål för vilka uppgifterna samlades in eller för vilka de senare behandlas. Detta återspeglas i 9 § personuppgiftslagen (första stycket punkten i). Den bestämmelsen gäller dock inte för de författningar som berörs av rambeslutet.

Skälen för bedömningen

Behövs det nya gallringsregler eller andra lagändringar?

Utgångspunkten i rambeslutet är densamma som i dataskyddsdirektivet, nämligen att personuppgifter av integritetsskäl inte får finnas tillgängliga längre tid än vad som krävs för ändamålet med behandlingen. Av det skälet ska det finnas i förväg bestämda frister för när olika typer av uppgifter ska gallras. Det överläts till

medlemsstaterna att avgöra hur långa gallringsfristerna ska vara, men utgångspunkten är att de inte får vara längre än nödvändigt. Huvudregeln är att gallringen ska leda till att uppgifterna raderas eller avidentifieras. Gallring kan också ske genom arkivering av uppgifterna.

De författningar som berörs av rambeslutet innehåller gallringsregler som har anpassats till de särskilda behoven inom respektive verksamhetsområde eller för det aktuella registret. Gallringsreglerna är därför utformade på olika sätt. Personuppgiftslagens generella föreskrift om att uppgifter som inte längre behövs för sitt ändamål ska gallras återspeglas i vissa författningar (se t.ex. 13 § polisdatalagen), men dessutom innehåller dessa särskilda gallringsregler för vissa register eller vissa typer av uppgifter. Kravet på att det ska finnas särskilt angivna gallringsfrister är således uppfyllt. Förslaget till ändrad lagstiftning för polisens behandling av personuppgifter innehåller också gallringsregler (Ds 2007:43 s. 261 ff.). Detsamma gäller förslaget om ny lagstiftning för Kustbevakningen (SOU 2006:18 s. 261 ff.) och förslaget till ny lagstiftning för domstolarna (SOU 2001:100 s. 164 ff.). Det sagda hindrar dock inte att det i fråga om enskilda författningar kan finnas anledning att överväga om gallringsfristerna behöver göras snävare eller om det krävs ändrade eller mer preciserade regler i fråga om gallring av vissa typer av uppgifter.

Den i rambeslutet anvisade möjligheten att gallra genom att arkivera i en separat miljö bör främst ses som en möjlighet att kunna dröja en tid efter gallringen innan uppgifterna lämnas vidare till myndighetens eget arkiv, till en arkivmyndighet eller förstörs slutligt. Det som är viktigt från integritetssynpunkt är att sådana uppgifter inte får användas i den brottsbekämpande verksamheten eller för någon av de andra verksamheter som ingår i rambeslutets tillämpningsområde.

Gallring av uppgifter i förundersökningar

Det bör dock framhållas att i fråga om förundersökningar görs såväl i polisdatalagen som i de författningar som reglerar personuppgiftsbehandlingen i Tullverkets, Kustbevakningens och Skatteverkets brottsbekämpande verksamhet undantag från de specifika gallringsreglerna. Uppgifter i förundersökningar gallras i stället enligt arkivlagstiftningen. I förarbetena till personuppgiftslagen framhölls att reglerna om sekretess och skydd för arkiv får anses utgöra sådana lämpliga skyddsåtgärder som krävs enligt dataskyddsdirektivet (prop. 1997/98:44 s. 48). Det finns inte skäl att nu göra någon annan bedömning. Rambeslutet tillåter, som framgått ovan, arkivering som ett alternativ till gallring och de nu aktuella reglerna får därför anses stå i överensstämmelse med detta.

Uppgifter om kvarstående misstankar

Sektorsförfattningarna för polisen, åklagarväsendet, Tullverket och Skatteverket innehåller också i stort sett likalydande bestämmelser om behandling av kvarstående misstankar. Reglerna i fråga föreskriver att, om en förundersökning har lagts ned på grund av bristande bevisning, får uppgifter om brottsmisstanken behandlas för annat ändamål än arkivering endast under förutsättning att

- den misstänkte enligt förundersökningsledarens bedömning fortfarande är skäligen misstänkt för brottet och
- uppgifterna behövs för att förundersökningen ska kunna tas upp på nytt.

Det kan ifrågasättas om dessa regler är förenliga med rambeslutets krav på gallring, eftersom utgångspunkten synes vara att uppgifterna alltjämt ska vara tillgängliga för behandling i den brottsbekämpande verksamheten. Reglerna i fråga anses också vara svårtolkade. Det kan därför finnas skäl att se över dem. Det kan anmärkas att det i förslaget till ny lagstiftning för polisens

personuppgiftsbehandling inte finns någon motsvarighet till dessa regler.

Underrättelse om nationella gallringsregler

Regleringen i artikel 10 skapar dels en möjlighet för översändande stat att underrätta mottagaren om sina gallringsfrister, dels en skyldighet att beakta andra staters gallringsfrister. Den förstnämnda bestämmelsen är viktig från integritetssynpunkt, eftersom den ger möjlighet att se till att våra svenska regler om gallring beaktas för den händelse den mottagande staten skulle ha längre gallringsfrister. Eftersom det inte är fråga om någon förpliktelse kräver artikeln i denna del inte någon lagändring. I det fortsatta arbetet får övervägas om det i förordningsform bör införas regler som ålägger svenska myndigheter att upplysa om våra gallringsregler. Det bör dock betonas att vårt system med förhållandevis komplexa gallringsregler, där fristen dels kan vara olika för skilda typer av uppgifter i ett och samma ärende, dels kan vara knuten till framtida händelser (t.ex. att det finns ett lagkraftätagande avgörande i ett svenskt brottmål) i det enskilda fallet kan bli mycket svåra att tillämpa för andra länders myndigheter. Det kan i sådana fall vara lämpligare att låta det mottagande landet tillämpa sina nationella regler för gallring. Mot den nu angivna bakgrunden förefaller det tveksamt om man bör införa någon direkt skyldighet att underrätta om svenska gallringsregler. Det får övervägas i det fortsatta arbetet om det är lämpligare att överlåta till tillämparen att avgöra när en sådan upplysning bör lämnas.

När det gäller förpliktelsen att beakta en annan stats gallringsregler får det anses vara ett sådant villkor för användningen av uppgifterna som behandlas i avsnitt 8.10. Sverige uppfyller således redan detta krav. Det kan emellertid finnas skäl att överväga om en erinran om systemet med användningsbegränsningar bör tas in i vissa författningar.

Sammanfattande bedömning

Den befintliga lagstiftningen uppfyller i och för sig kraven i rambeslutet på att det ska finnas gallringsfrister. Det kan ändå finnas skäl att i det fortsatta arbetet se över gallringsreglerna i vissa författningar. Det kan t.ex. behövas närmare överväganden om gallringsreglerna behöver göras snävare eller om det krävs större precisering i fråga om gallringen av vissa typer av uppgifter eller annan ändring i dessa. Det kan också finnas skäl att överväga i vilken utsträckning gallringsregler bör finnas i lag eller i lägre författning.

8.10 Användningsbegränsningar

Bedömning: De befintliga reglerna om begränsning av användningen av information eller bevismaterial som erhållits från en annan stat är tillräckliga. För de myndigheter som inte enbart agerar med stöd av de lagar som har regler om användningsbegränsning bör möjligheten att införa en motsvarande reglering övervägas. Vidare bör några lagar kompletteras med regler som ger svenska myndigheter samma rätt att ställa villkor för användningen när information eller bevismaterial lämnas från Sverige till en annan stat.

Innehållet i rambeslutet

Om det gäller särskilda restriktioner för behandlingen av uppgifter enligt den översändande statens lagstiftning ska, enligt *artikel 13*, den sändande staten underrätta mottagaren om restriktionerna. Mottagaren ska se till att dessa restriktioner följs. Medlemsstaterna får inte tillämpa några andra restriktioner när det gäller överföring av uppgifter till en annan stat än som gäller motsvarande nationella överföringar. Artikeln har inte någon motsvarighet i dataskyddsdirektivet.

Regler om användningsbegränsningar

Svensk lagstiftning innehåller regler för hantering av information eller bevismaterial som erhålls från en utländsk myndighet med villkor för användningen, s.k. användningsbegränsningar. Principen är att sådana villkor tar över vad som annars gäller enligt svensk rätt. Det innebär t.ex. att åtalsplikten inte gäller.

Som redovisats närmare i avsnitten 5.2 och 5.3 finns det bestämmelser om användningsbegränsningar i lagen om internationell rättslig hjälp i brottmål (5 kap. 1 §), lagen om internationellt polissamarbete (3 §), lagen om internationellt samarbete i brottsutredningar (5, 13 och 16 §§), lagen om internationellt tullsamarbete (4 kap. 2 §) samt lagen om Schengens informationssystem (10 §). I samtliga lagar föreskrivs att svenska myndigheter är skyldiga att följa de villkor som ställs av en utländsk myndighet eller mellanfolklig organisation.

Bara vissa av lagarna (t.ex. lagen om internationell rättslig hjälp i brottmål) innehåller regler om en svensk myndighets rätt att ställa motsvarande villkor för användningen av information eller bevismaterial som överlämnas av Sverige till en annan stat.

Användningen av överskottsinformation

Något som understryker behovet av regler som gör det möjligt för svenska myndigheter att ställa villkor om användningen av material som överlämnas till en annan stat är bestämmelserna om användning av överskottsinformation från vissa hemliga tvångsmedel. Med överskottsinformation avses att en myndighet vid användning av ett tvångsmedel får uppgifter om ett annat brott än det som legat till grund för tvångsmedelsbeslutet.

Genom prop. 2004/05:143 infördes bestämmelser som begränsar möjligheten att använda överskottsinformation från vissa hemliga tvångsmedel. Regleringen innebär att sådan överskottsinformation som härrör från hemlig teleavlyssning endast får användas i vissa i 23 kap. 23 a § rättegångsbalken specificerade

situationer. Uppgifter om förestående brott får utan begränsningar användas för att förhindra det nya brottet. Uppgifter om begångna brott får användas för att utreda brottet om en utredning redan pågår. Däremot får förundersökning för det nya brottet inledas endast om det för brottet är föreskrivet fängelse i ett år eller däröver och det kan antas att påföljden inte stannar vid böter, eller om det finns särskilda skäl. En motsvarande reglering för användning av överskottsinformation från hemlig kameraövervakning finns i 6 a § lagen (1995:1506) om hemlig kameraövervakning.

När lagen (2007:978) om hemlig rumsavlyssning och lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott infördes, reglerades användningen av överskottsinformation på likartat sätt i dessa lagar. Den regleringen är dock strängare, eftersom överskottsinformation bara får användas för att utreda brott som i sig hade kunnat föranleda användning av det aktuella tvångsmedlet. Överskottsinformation får dock alltid användas för att förhindra nya brott.

Skälen för bedömningen

Behövs det nya eller ändrade regler?

Som framgått i avsnitt 5.2 finns det numera inte någon generell regel om användningsbegränsning vid internationellt samarbete i brottmål. Reglerna om att svenska myndigheter ska iakttä användningsbegränsningar gäller för information som erhålls vid internationellt polissamarbete, internationellt tullsamarbete eller rättslig hjälp. Information som mottas på detta sätt av polisen, åklagare, Tullverket och Kustbevakningen täcks således. Vidare täcks den information som kommit genom sådana kanaler och som därefter kommer någon av de nämnda myndigheterna eller Skatteverket, domstolsväsendet eller kriminalvården till del. För de två sistnämnda verksamhetsområdena torde det inte behövas någon ytterligare lagstiftning, bl.a. av det skälet att det i dessa

verksamheter sällan torde finnas något behov av att kunna använda uppgifterna för något annat ändamål än det för vilket de har översänts.

Däremot kan det ifrågasättas om det inte, för den händelse Skatteverket i sin brottsbekämpande verksamhet mottar information direkt från en motsvarande myndighet i en annan stat, bör finnas en reglering som motsvarar vad som gäller för övriga brottsbekämpande myndigheter. För Skatteverkets del finns redan sådan reglering när uppgifter erhålls för beskattningsändamål. Det är vidare osäkert om regleringen för Kustbevakningen är heltäckande. Även om myndigheten enligt svensk lagstiftning är behörig myndighet enligt både lagen om internationellt polissamarbete och lagen om internationellt tullsamarbete är det inte självklart att dess motsvarigheter i andra länder har status som behörig myndighet och att den nuvarande lagstiftningen i alla situationer täcker sådan information som lämnas direkt från en sådan myndighet till Kustbevakningen. Den frågan får övervägas i det fortsatta arbetet.

Vidare torde det krävas ytterligare lagstiftning när det gäller svenska myndigheters rätt att ställa villkor för användningen, om de översänder information eller bevismaterial till en annan stat. Sett ur integritetssynpunkt är den frågan minst lika viktig som att vi följer utländska villkor.

För en svensk myndighet är möjligheten att ställa villkor för användningen särskilt viktig i två situationer. Den ena är när användningen har betydelse för en pågående svensk brottsutredning eller lagföring eller för pågående svenskt underrättelsearbete. Då kan det vara nödvändigt att ställa villkor som anger när och hur materialet får användas eller som villkorar användningen på så sätt att det krävs kontakt med svensk myndighet innan det får användas. Den andra situationen är när svensk rätt begränsar rätten att hantera materialet. I förarbetena till införandet och ändringar i lagen om internationell rättslig hjälp i brottmål har framhållits att det är lämpligt att kräva att material från hemlig teleavlyssning förstörs när utredningen eller lagföringen är avslutad i den andra staten (se prop. 1999/2000:61 s. 201 och prop.

2004/05:144 s. 170). Ett sådant villkor innebär att materialet ska hanteras på sätt som motsvarar bestämmelserna i 27 kap. 24 § rättegångsbalken. Denna paragraf, och motsvarande bestämmelse i lagen (1995:1506) om hemlig kameraövervakning, får anses vara en sådan särskild restriktion som avses i artikel 13.

De begränsningar i fråga om användning av överskottsinformation som gäller för svenska myndigheter får också anses vara sådana särskilda restriktioner som anges i artikel 13. Restriktionerna för användningen av sådant material bör givetvis gälla i samma utsträckning om det lämnas över till en utländsk myndighet som till en svensk. Mot den bakgrunden är det viktigt att det finns regler som gör det möjligt att ställa sådana villkor. De lagar som enbart innehåller en reglering av användningen av mottaget material bör således kompletteras med bestämmelser som möjliggör för en svensk myndighet att ställa villkor när information eller material lämnas över till en annan stat.

En annan fråga som måste uppmärksammas är spontant uppgiftslämnande. Vissa av reglerna om användningsbegränsning är utformade så att det står klart att även villkor som ställs i samband med att uppgifter överlämnas spontant är bindande (se t.ex. 5 kap. 1 § andra stycket lagen om internationell rättslig hjälp i brottmål), medan det i andra fall är mera osäkert om spontant lämnade uppgifter skyddas på samma sätt som uppgifter som lämnas på begäran. Rambeslutets tillämpningsområde omfattar både uppgifter som lämnas spontant och uppgifter som lämnas på begäran. I de fall där det kan vara osäkert om en regel om användningsbegränsning även täcker spontant lämnade uppgifter får det övervägas i det fortsatta arbetet om det krävs ändringar i förtydligande syfte.

Det kan anmärkas att frågan om användningsbegränsningar aktualiseras vid genomförandet av andra EU-instrument, bl.a. rambeslutet om en europeisk bevisinhämtningsorder och VIS-rådsbeslutet.

Sammanfattande bedömning

De befintliga reglerna om användningsbegränsningar är tillräckliga. Däremot bör tillses att svenska myndigheter alltid har möjlighet att ställa villkor för användningen av information eller bevismaterial som överlämnas till en annan stat, när det är motiveerat i ett enskilt fall. För de myndigheter som inte agerar enbart med stöd av de lagar som redan innehåller användningsbegränsningar bör regleringen ses över.

8.11 Information till den registrerade

Bedömning: Den nuvarande lagstiftningen uppfyller i princip kraven i rambeslutet. I någon enstaka författning kan en ändring vara nödvändig.

Innehållet i rambeslutet

Medlemsstaterna ska enligt *artikel 16* i rambeslutet se till att den registrerade enligt nationell rätt informeras om förekommande insamling eller behandling av personuppgifter. Vilka former informationen ska ha bestäms av medlemsstaterna. Det kan göras t.ex. genom lagstiftning eller offentliggörande av vilka typer av uppgiftsbehandling som förekommer (skäl 13 a). Har personuppgifter överförts till eller gjorts tillgängliga mellan medlemsstaterna får varje stat, i enlighet med sin nationella lagstiftning, begära att den andra staten inte informerar den registrerade. Den mottagande staten ska då inte informera den registrerade utan förhandsmedgivande från den andra staten.

Enligt *artikel 17* punkten 1 har varje registrerad person rätt att på begäran, med rimliga intervall, utan hinder och utan större tidsutdräkt eller kostnader få åtminstone

- bekräftelse från den registeransvarige eller från den nationella tillsynsmyndigheten på om uppgifter om honom eller

henne har överförts till eller gjorts tillgängliga för en annan stat, eller annan mottagare som anges i rambeslutet, samt information om till vilka mottagare eller kategorier av mottagare som uppgifter lämnats och information om vilka uppgifter som behandlas, eller

- bekräftelse från den nationella tillsynsmyndigheten på att alla nödvändiga kontroller har utförts.

Medlemsstaterna har enligt punkten 2 rätt att begränsa åtkomsten enligt det första alternativet i punkten 1, om begränsningen med beaktande av vederbörandes legitima intressen är en nödvändig och rimlig åtgärd för att

- a) inte försvåra officiella och rättsliga förfrågningar, brottsutredningar eller förfaranden,
- b) inte skada förebyggande, upptäckt, utredning eller lagföring av brott eller verkställighet av straffrättsliga påföljder,
- c) för att skydda den allmänna säkerheten,
- d) för att skydda nationell säkerhet, eller
- e) för att skydda den registrerades eller andra personers fri- och rättigheter.

En vägran att lämna information ska enligt huvudregeln vara skriftlig och innehålla skälen för vägran. Grundas vägran på någon av punkterna a–e ovan behöver någon underrättelse inte lämnas. Under alla förhållanden ska den registrerade underrättas om att han eller hon kan klaga till den nationella tillsynsmyndigheten, en rättslig myndighet eller till domstol.

Personuppgiftslagen

Dataskyddsdirektivet innehåller också bestämmelser om information till den registrerade, närmare bestämt artiklarna 10 och 11. I direktivet skiljs, på samma sätt som i rambeslutet, mellan information som ska lämnas när uppgifterna samlas in och information som ska lämnas på den registrerades egen begäran. Bestämmelserna återspeglas i 23–26 §§ personuppgiftslagen, där 23 och 24 §§ reglerar sådan information som ska lämnas själv-

mant samt 25 och 26 §§ sådan information som ska lämnas efter begäran. Ett generellt undantag görs i 27 § personuppgiftslagen, där det föreskrivs att om det i annan lag eller författning finns regler om att uppgifter inte får lämnas ut gäller dessa framför personuppgiftslagens regler. Bestämmelser om sekretess och tystnadsplikt gäller således framför informationsplikten.

Enligt 6 § lagen om personuppgiftsbehandling i Tullverkets brottsbekämpande verksamhet gäller de nu aktuella bestämmelserna, med undantag för 24 § personuppgiftslagen. Varken polisdatalagen eller någon av de övriga sektorsförfattningar som berörs av rambeslutet innehåller särskilda bestämmelser om information till den registrerade. Bestämmelserna i 23–26 §§ personuppgiftslagen gäller således. Vissa registerförfattningar har inte heller några regler om information till den registrerade. Även i de fallen torde 23–26 §§ gälla.

Skälen för bedömning

Behövs det nya regler om information?

Regleringen i personuppgiftslagen innebär att information ska lämnas i betydligt större omfattning än vad som krävs i rambeslutet. Kraven i artikel 17 är således redan uppfyllda i de fall där personuppgiftslagen är tillämplig. Eftersom artikel 16 enbart innehåller krav på att det ska finnas nationella regler om information till den registrerade uppfyller Sverige kraven även i denna del.

I författningarna om enskilda register finns i vissa fall särskilda regler om information till den registrerade.

Enligt 9 § lagen om belastningsregister har en enskild rätt att på begäran skriftligen få del av samtliga uppgifter ur registret om sig själv. Sådana uppgifter ska lämnas på begäran utan avgift en gång per kalenderår. Vidare anges vissa andra situationer där den enskilde har rätt till registerutdrag. Bestämmelsen är något

annorlunda utformad än motsvarande regel i personuppgiftslagen, men får anses uppfylla kraven i rambeslutet.

Lagen om misstankeregister innehåller också bestämmelser om utlämnande av uppgifter till enskilda. Den registrerade själv tillhör inte dem som har rätt till information. Detta bör ses mot bakgrund av dels att rätten till information för brottsmisstänka regleras i rättegångsbalken (23 kap. 18 och 21 §§), dels att information i många fall skulle skada den brottsbekämpande verksamheten. Att inte lämna information till den registrerade om uppgifter i misstankeregistret är således väl förenligt med de undantag som anges i artikel 17 punkten 2 a–c. Särregleringen torde därför uppfylla kraven i rambeslutet.

Även lagen om internationellt tullsamarbete innehåller en särskild bestämmelse om information. Enligt 2 kap. 8 § är en svensk myndighet som har sänt över en uppgift till en utländsk myndighet eller mellanfolklig organisation skyldig att, på begäran av den som uppgiften rör, underrätta denne om vilken utländsk myndighet eller organisation som uppgiften översänts till och för vilket ändamål. Någon underrättelse behöver dock inte lämnas om det är uppenbart obehövt eller om det kan befaras att underrättelsen skulle försvåra mottagarens utredning eller beslut i ärendet. Om det gäller sekretess enligt 5 kap. 1 § sekretesslagen för uppgiften behöver någon underrättelse inte heller lämnas. De flesta av dessa begränsningar torde rymmas inom de ramar som anges i artikel 17 punkten 2. Det kan däremot diskuteras om undantaget från skyldigheten att underrätta när det är uppenbart obehövt är förenligt med rambeslutet, som inte gör något sådant undantag. Den konvention som lagstiftningen bygger på hänvisar enbart till nationell rätt och innehåller alltså inte heller något sådant undantag. Frågan bör uppmärksammas i det fortsatta arbetet.

En annan fråga är om rambeslutet bör föranleda att det införs en särskild reglering av rätten till information i sektorsförfattningarna, som tydligare ger uttryck för regleringen i rambeslutet. Detta skall ses mot bakgrund av regleringen i 24 § personuppgiftslagen, som ålägger den personuppgiftsansvarige att, i de fall

där uppgifterna har samlats in från någon annan källa än den registrerade, självant informerades den registrerade om behandlingen. Detta gäller dock inte om det finns särskild reglering. Enligt förslagen till ny lagstiftning för polisen, Kustbevakningen och domstolarna ska 24 § personuppgiftslagen inte gälla i deras verksamhet. Något behov av information om sådan behandling av personuppgifter som regleras i särskild lagstiftning har inte bedömts föreligga. Som nyss nämnts gäller 24 § personuppgiftslagen inte för Tullverket. Det finns skäl att överväga motsvarande begränsning i övriga sektorslagar.

Den sekretess som gäller för uppgifter i aktuella register är väl förenlig med undantaget i artikel 17 punkten 2 e.

I sammanhanget bör också Säkerhets- och Integritetsskyddsnämnden nya roll nämnas. Nämnden har, som redovisats i avsnitt 4.7.2, till främsta uppgift att övervaka hanteringen av hemliga tvångsmedel men ska även kontrollera Säkerhetspolisens personuppgiftsbehandling. Dessutom kan enskilda vända sig till nämnden och begära att den kontrollerar om den enskilde blivit felbehandlad av Säkerhetspolisen. I förslaget till ny reglering av polisens personuppgiftsbehandling föreslås nämnden få till uppgift att övervaka behandlingen av personuppgifter inom hela polissektorn, särskilt avseende behandling av känsliga personuppgifter (se Ds 2007:43 s. 334 ff.).

Mot den nu angivna bakgrunden ter det sig naturligt att vid utformningen av framtida regler om information till den registrerade överväga hur nämndens roll bör se ut, för att skapa bra möjligheter till kontroll av personuppgiftsbehandlingen även inom delar av samhället där insynen är begränsad på grund av sekretessregleringen.

Artikel 16 punkten 2 innehåller en förpliktelse att, om en annan stat begär det, inte lämna någon information till den registrerade. En begäran om detta får anses vara ett sådant villkor för användningen av uppgifter som har berörts i avsnitt 8.10. Den nuvarande lagstiftningen är således tillräcklig. För att underlätta tillämpningen skulle det dock vara en fördel om bestämmelsen i

fråga antingen fanns i samma författning som reglerna om information eller anmärktes genom en hänvisning.

Sammanfattande bedömning

Den nuvarande lagstiftningen om behandling av personuppgifter uppfyller i allt väsentligt kraven i rambeslutet. Även om det finns regler som täcker rambeslutets krav, kan det vara lämpligt att i det fortsatta arbetet närmare överväga en särreglering för de aktuella myndigheterna när det gäller informationen till den registrerade.

8.12 Tillgång till rättsmedel

Bedömning: De flesta författningar innehåller regler om överklagande som uppfyller rambeslutets krav på att den enskilde ska ha möjlighet att vända sig till domstol. I de fall där möjlighet till överklagande saknas torde det krävas ändrad reglering. Genom rätten till överklagande och de övriga möjligheter som finns till prövning av felaktig personuppgiftsbehandling torde kraven i rambeslutet vara uppfyllda.

Innehållet i rambeslutet

I *artikel 20* föreskrivs att den registrerade ska ha rätt att, utan att det påverkar möjligheten att utnyttja något administrativt förfarande, inför domstol föra talan mot kränkningar av sådana rättigheter som skyddas av rambeslutet.

Personuppgiftslagen

Bestämmelsen har sin motsvarighet i artikel 22 i dataskyddsdirektivet. Rätten till överklagande av myndighets beslut om information och rättelse regleras i 52 § personuppgiftslagen. Enligt paragrafen får en myndighets beslut om information enligt bl.a. 26 § och om rättelse enligt 28 § överklagas till allmän förvaltningsdomstol. Bestämmelsen gäller dock inte i de fall där det finns avvikande regler om överklagande i den särskilda författningen. Sådana finns bl.a. för domstolsväsendet och kriminalvården. Tanken bakom den generella regeln om överklagande är att man inte längre behöver ha regler om överklagande i särskilda registerförfattningar. Så länge dessa regler inte har upphävts gäller de dock framför personuppgiftslagen. Regeringen framhöll i lagstiftningsärendet att det finns anledning att särskilt uppmärksamma frågan om det behövs regler om överklagande vid översyn av registerförfattningar (prop. 2005/06:173 s. 53).

Skälen för bedömningen*Regler om överklagande*

Genom 52 § personuppgiftslagen är det numera väl sörjt för att myndighetsbeslut som rör rätten till information (registerutdrag) enligt 26 § personuppgiftslagen och rätten till rättelse av personuppgifter kan överklagas. Eftersom varken polisdatalagen eller någon av de andra särskilda författningar som reglerar register i polisverksamheten innehåller några bestämmelser om överklagande gäller 52 § personuppgiftslagen.

I de författningar som gäller för de andra verksamhetsområden som berörs av rambeslutet finns särskilda bestämmelser om överklagande som med ett undantag i sak ger samma rätt till överklagande som 52 § personuppgiftslagen. I dessa fall uppfyller Sverige redan kraven i rambeslutet. Det kan dock i det fortsatta arbetet finnas skäl att överväga om de särskilda reglerna om

överklagande bör upphävas, eftersom de i de flesta fall inte fyller något faktiskt behov, samtidigt som de i vissa fall begränsar den enskildes rätt att överklaga. Det finns även andra skäl som talar för att reglerna om överklagande bör ses över.

En författning, den som gäller för Skatteverkets behandling av personuppgifter vid medverkan i brottsutredningar, innehåller en särskild bestämmelse om överklagande som dock inte omfattar överklagande av bristande information från den personuppgiftsansvarige. Här torde det således krävas lagändring för att Sverige ska uppfylla kraven i rambeslutet.

Lagen om Schengens Informationssystem innehåller, som tidigare nämnts, en särskild regel om rättelse men ingen regel om överklagande. Numera torde därför 52 § personuppgiftslagen vara tillämplig, eftersom den är generellt utformad. Som framhållits i prop. 2006/07:33 s. 32 om godkännande av rådsbeslutet om andra generationen av Schengens informationssystem kan det dock vara lämpligt att se över lagen på denna punkt. Det kan därför antas att ett förslag om lagändring aktualiseras vid genomförandet av rådsbeslutet.

När det gäller de särskilda bestämmelserna om överklagande i domstolsväsendets författningar har regeringen tidigare framhållit att det även i fortsättningen torde krävas särreglering och hänvisat till det pågående arbetet med ny lagstiftning på området (prop. 2005/06:173 s. 52). Även för kriminalvårdens del kan det finnas skäl att ha kvar särregleringen.

Andra möjligheter till prövning

Utöver möjligheten att överklaga beslut av en personuppgiftsansvarig myndighet finns det även andra möjligheter att agera för den som känner sig förfördelad av hur behandlingen av personuppgifter rörande honom eller henne har skötts. I avsnitt 8.15 behandlas de befogenheter som Datainspektionen har i egenskap av tillsynsmyndighet. Varje medborgare kan vända sig dit med klagomål.

En annan möjlighet är att begära skadestånd av staten för skada som någon anställd har vållat i sin myndighetsutövning. Frågor om skadestånd för felaktig personuppgiftsbehandling behandlas i avsnitt 8.16.

Utgör den felaktiga handläggningen brottslig gärning har även en enskild person rätt att väcka åtal mot en tjänsteman som han anser gjort sig skyldig till brottsligt handlande.

Vidare kan varje medborgare vända sig till Riksdagens ombudsmän (JO) med klagomål. Om JO finner att fel har begåtts kan han rikta kritik mot myndigheten eller tjänstemannen eller väcka fråga om disciplinärt ansvar. Om det felaktiga handlandet utgör brott kan JO väcka åtal för detta.

Sammanfattande bedömning

Genom de ovan redovisade möjligheterna, framför allt rätten till överklagande, får den nuvarande lagstiftningen anses uppfylla kraven i rambeslutet. I de författningar där möjlighet till överklagande saknas torde det krävas ändrad reglering.

8.13 Säkerheten vid behandlingen

Bedömning: Reglerna i personuppgiftslagen om säkerhet vid behandlingen får, mot bakgrund av tidigare ställningstaganden, anses vara tillräckliga. Några lagregler därutöver torde inte krävas.

Innehållet i rambeslutet

I *artikel 22* punkterna 1, 3 och 4 regleras säkerheten vid behandling av personuppgifter. Artikel 22 ålägger medlemsstaterna att se till att behöriga myndigheter vidtar lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifter från att av-

siktligt eller oavsiktligt utplånas eller gå förlorade samt från ändringar, otillåten spridning och otillåten tillgång till uppgifterna. I punkten 2 ställs mera konkreta krav på olika typer av åtgärder som dels ska förhindra att uppgifterna hamnar i orätta händer, dels tillförsäkra att det går att i efterhand kontrollera vem som har lagt in uppgifter och att de system som används fungerar tillfredsställande.

Enligt *artikel 11* punkten 1 ska varje överföring av personuppgifter registreras eller dokumenteras för att möjliggöra kontroll av behandlingen i efterhand.

I sak motsvarande krav ställs bl.a. i Europolkonventionen och Schengenkonventionen.

Personuppgiftslagen

I artiklarna 16 och 17 i dataskyddsdirektivet finns motsvarande, men mer generella bestämmelser om säkerhet vid behandlingen av personuppgifter. Dessa återspeglas i svensk rätt genom 30 och 31 §§ personuppgiftslagen. Vidare föreskrivs i 32 § personuppgiftslagen att tillsynsmyndigheten får besluta om säkerhetsåtgärder enligt 31 §.

Bestämmelserna i 30–32 §§ personuppgiftslagen får anses tillämpliga inom de verksamhetsområden som berörs av rambeslutet. I 6 § lagen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet finns en direkt hänvisning till bestämmelserna i 30–32 §§ personuppgiftslagen. En motsvarande hänvisning föreslås i lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet (Ds 2007:47 s. 117). Motsvarande förslag finns för Kustbevakningens personuppgiftsbehandling (SOU 2006:18 s. 198) och för domstolsväsendets (SOU 2000:100 s. 109).

Ingen av de lagar som reglerar enskilda register innehåller några bestämmelser om datasäkerhet, varför 30–32 §§ personuppgiftslagen får anses vara tillämpliga på dessa.

Skälen för bedömningen

När Schengenkonventionen genomfördes i svensk rätt gjordes bedömningen att Sverige genom de allmänna skyddsreglerna i personuppgiftslagen uppfyllde de säkerhetskrav som konventionen ställde (jfr prop. 1999/2000:64 s. 148). Konventionens krav på datasäkerhet har – också i fråga om detaljer rörande vilka enskilda säkerhetsåtgärder som krävs – stor likhet med de krav som ställs i rambeslutet. Även när det gäller motsvarande bestämmelser i det rådsbeslut som kommer att ersätta Schengenkonventionens bestämmelser om Schengens informationssystem har regeringen gjort den preliminära bedömningen att det inte krävs några författningsändringar (prop. 2006/07:33 s. 11 f.). Motsvarande bedömning gjordes i fråga om kraven på datasäkerhet i Europokonventionen (se prop. 1996/97:164).

Mot den nu angivna bakgrunden bedöms artikel 22 inte kräva några lagstiftningsåtgärder. Huruvida det kan behövas närmare regler i förordning får bedömas under det fortsatta arbetet.

8.14 Sekretess

Bedömning: Det behövs inga nya bestämmelser om sekretess eller tystnadsplikt.
--

Innehållet i rambeslutet

I *artikel 21* i rambeslutet föreskrivs att personuppgifter endast får behandlas av anställda vid den behöriga myndigheten eller efter instruktioner från denna, om det inte föreligger rättsliga skyldigheter till annan behandling. Vidare ska den som anlitas för att arbeta för en behörig myndighet vara bunden av alla de bestämmelser om skydd av uppgifter som gäller för respektive myndighet.

Enligt *artikel 25* punkten 4 ska tillsynsmyndighetens ledamöter och personal vara bundna av tystnadsplikt rörande uppgifter de fått del av i tjänsten även sedan anställningen eller uppdraget har upphört.

Personuppgiftslagen

Artikel 21 har sin motsvarighet i artikel 16 i dataskyddsdirektivet. Den har genomförts genom 30 § i personuppgiftslagen som, något förenklat, föreskriver att den som arbetar med personuppgiftsbehandling ska göra detta i enlighet med instruktioner från den personuppgiftsansvarige. Det ska finnas ett skriftligt avtal som anger detta. Om det i lag eller annan författning finns särskilda bestämmelser om behandling av personuppgifter i det allmännas verksamhet gäller i stället dessa.

I fråga om Tullverkets personuppgiftsbehandling hänvisas till den bestämmelsen. En motsvarande hänvisning föreslås i fråga om polisens (Ds 2007:43 s. 117) och Kustbevakningens (SOU 2006:18 s. 198) framtida personuppgiftsbehandling. Paragrafen torde vara tillämplig på övriga författningar.

Skälen för bedömningen

Sekretesslagen ger, som framgått av redovisningen i avsnitt 4.8, ett bra skydd för den registrerade vid behandling som äger rum i det allmännas verksamhet. Att den tystnadsplikt som gäller i fråga om sekretessbelagda uppgifter gäller även efter det att en person har lämnat sin anställning eller sitt uppdrag följer av 1 kap. 6 § sekretesslagen. Några nya bestämmelser om sekretess bedöms därför inte vara nödvändiga med anledning av artikel 25.

När det gäller innehållet i artikel 21 bör framhållas att i det allmännas verksamhet kan disciplinärt ansvar utkrävas av en arbetstagare som uppsåtligen eller av oaktsamhet åsidosätter vad som gäller för anställningen; se 14 § lagen (1994:260) om offent-

lig anställning. Detta torde utgöra en tillräcklig garanti för att anställda följer regelverket vid behandlingen av personuppgifter.

Det finns, utöver förbudet i 21 § personuppgiftslagen mot att behandla uppgifter om lagöverträdelse, inte något formellt hinder mot att låta viss behandling av personuppgifter ske utanför en myndighet. Arten av de verksamheter som omfattas av rambeslutet är dock sådan att utrymmet för att låta behandla personuppgifter utanför myndighetssfären torde vara mycket begränsat. Det som möjligen kan komma i fråga torde vara teknisk bearbetning i någon form. Sådan bearbetning måste uppfylla säkerhetskraven i 30 och 31 §§ personuppgiftslagen.

Inte heller artikel 21 torde således inte kräva någon lagstiftningsåtgärd.

8.15 Tillsyn

Bedömning: De bestämmelser som redan finns om tillsynsmyndigheternas befogenheter är tillräckliga för att uppfylla förpliktelseerna i rambeslutet. Datainspektionen bör utses till nationell tillsynsmyndighet. Säkerhets- och Integritetskyddsnämnden bör, vid sidan av Datainspektionen, i fråga om polisens verksamhet, ges ställning som nationell tillsynsmyndighet inom sitt verksamhetsområde.

Innehållet i rambeslutet

Enligt *artikel 25* i rambeslutet ska varje medlemsstat utse en eller flera tillsynsmyndigheter att övervaka tillämpningen av de bestämmelser som antas i enlighet med rambeslutet. Myndigheterna ska vara oberoende när de fullgör sina åligganden. Tillsynsmyndigheten ska ha vissa befogenheter, nämligen

- utredningsbefogenheter, inkluderande rätt att få tillgång till de uppgifter som behandlas och all nödvändig information som behövs för att utföra tillsynen,
- faktiska befogenheter att ingripa, samt
- befogenhet att inleda rättsliga förfaranden.

Var och en ska ha rätt att vända sig till tillsynsmyndigheten i frågor som rör behandling av personuppgifter.

I *artikel 11* punkten 2 föreskrivs att den nationella tillsynsmyndigheten ska få tillgång till registrering och dokumentation som rör behandlingen av personuppgifter.

Vidare föreskrivs i *artikel 23* att den nationella tillsynsmyndigheten ska rådfrågas innan behandling av personuppgifter i nya register påbörjas, dels om känsliga personuppgifter kommer att behandlas, dels om typen av behandling, särskilt användning av nya teknik eller nya förfaranden som innebär speciella risker för registrerades grundläggande fri- och rättigheter och deras rätt till privatliv.

Artikel 23 innehåller således inte, som artikel 20 i dataskyddsdirektivet, uttryckligt krav på anmälan av särskilt integritetskänsliga behandlingar för förhandskontroll av tillsynsmyndigheten. Under förhandlingsarbetet har också gjorts klart att artikel 23 endast innebär förpliktelser av det slag som anges i artikel 28 punkten 2 i dataskyddsdirektivet. Tolkad på detta sätt ålägger den alltså inte medlemsstaterna att ha ett system med obligatorisk förhandskontroll av enskilda register utan tillsynsmyndighetens möjlighet att påverka kan tillgodoses på annat sätt, t.ex. genom att myndigheten får möjlighet att yttra sig i ett lagstiftningsärende. Eftersom medlemsstaterna har rätt att föreskriva strängare regler hindrar artikeln å andra sidan dem inte från att ha ett system med kontroll på förhand i fråga om enskilda register eller liknande.

Personuppgiftslagen

Innehållet i artiklarna motsvarar i sak vad som gäller enligt artikel 28 punkterna 1 och 2 samt del av punkten 3 i dataskyddsdirektivet. Dessa har genomförts i svensk rätt genom 43–47 §§ personuppgiftslagen.

Enligt 43 § har inspektionen rätt att för sin tillsyn på begäran få tillgång till de personuppgifter som behandlas, upplysningar om och dokumentation av behandlingen av personuppgifter och säkerheten vid denna samt tillträde till sådana lokaler som har anknytning till behandlingen av personuppgifter. I 44–46 §§ personuppgiftslagen regleras tillsynsmyndighetens rätt att förelägga vite för att framtvunga rättelse. Enligt 47 § får tillsynsmyndigheten ansöka hos allmän förvaltningsdomstol om att personuppgifter som har behandlats på olagligt sätt ska utplånas.

Skälen för bedömningen*Tillsynsmyndighetens befogenheter*

När det gäller tillsynsmyndighetens befogenheter innehåller rambeslutet, som framgått ovan, inte några krav på andra befogenheter än de som dataskyddsdirektivet förutsätter. Dessa återspeglas i personuppgiftslagen och gäller i allt väsentligt för de verksamheter som omfattas av rambeslutets tillämpningsområde. Någon ytterligare lagstiftning krävs därför inte.

I fråga om motsvarigheten till artikel 23 ansåg regeringen att det inte krävdes någon lagreglering när dataskyddsdirektivet genomfördes i svensk lagstiftning. Detta motiverades med att det i 7 kap. 2 § regeringsformen föreskrivs att behövliga upplysningar ska hämtas in vid beredningen av regeringsärenden samt att man kunde utgå från att riksdagen på likartat sätt skaffar sig det beredningsunderlag som krävs innan den tar initiativ till ny lagstiftning (prop. 1997/98:44 s. 101). Det finns inte skäl att nu göra någon annan bedömning av lagstiftningsbehovet.

Vem ska vara tillsynsmyndighet?

Eftersom Datainspektionen redan har uppgiften som nationell tillsynsmyndighet enligt dataskyddsdirektivet är det naturligt att myndigheten får samma roll enligt rambeslutet (jfr skäl 16 a).

Som redovisats i avsnitt 4.7.2 har den nyinrättade Säkerhets- och integritetsskyddsnämnden vissa tillsynsuppgifter när det gäller Säkerhetspolisens personuppgiftsbehandling. I förslaget till ny lagstiftning om polisens personuppgiftsbehandling föreslås nämnden få en utökad roll i form av tillsyn över den övriga polisens personuppgiftsbehandling. Som redovisats i avsnitt 8.11 innehåller rambeslutet särskilda bestämmelser om den registrerades rätt till information. Den registrerade har rätt att åtminstone få besked om att det har gjorts en kontroll av att personuppgifterna om honom eller henne har behandlats korrekt. Detta motiverar att även Säkerhets- och integritetsskyddsnämnden utpekas som en nationell tillsynsmyndighet inom sitt verksamhetsområde. Det torde framför allt vara på polisens område som mängden sekretessbelagd information som inte kan delges den informerade är störst. Då kan det finnas särskilda skäl att, som en extra rättssäkerhetsgaranti, låta registrerade kunna vända sig till nämnden för att åtminstone få kontrollerat att personuppgifter om dem har behandlats korrekt.

Säkerhets- och integritetsskyddsnämndens befogenheter regleras i lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet. Enligt 4 § har nämnden rätt att av förvaltningsmyndigheter få de uppgifter och det biträde som nämnden begär. Även domstolar och förvaltningsmyndigheter som inte omfattas av tillsynen är skyldiga att lämna nämnden de uppgifter den begär. Av förarbetena framgår att nämnden ska utöva sin tillsyn genom inspektioner (prop. 2006/07:133 s. 68 f.). Eftersom Säkerhets- och integritetsskyddsnämnden endast ska utöva sin tillsyn vid sidan av Datainspektionen, får nämndens befogenheter anses vara tillräckliga. Någon lagstiftningsåtgärd är därför inte påkallad.

8.16 Skadestånd

Bedömning: De flesta av författningarna uppfyller kraven i rambeslutet eftersom de hänvisar till personuppgiftslagens reglering av skadeståndsansvar. I några fall torde krävas kompletterande regler.

Innehållet i rambeslutet

Enligt *artikel 19* i rambeslutet har den som har lidit skada till följd av en otillåten behandling av personuppgifter eller någon annan åtgärd som är oförenlig med nationell lagstiftning rätt till ersättning av den registeransvarige eller annan myndighet för den skada som han eller hon har lidit. I fråga om översända uppgifter kan mottagaren inte åberopa att dessa var felaktiga för att undgå ansvar. Däremot kan mottagaren i vissa fall ha regressrätt mot den översändande för det skadestånd som betalats ut.

Personuppgiftslagen

En motsvarande reglering finns i artikel 23 punkten 1 i dataskyddsdirektivet, som har genomförts i svensk rätt genom 48 § personuppgiftslagen. Skadeståndsansvaret enligt den paragrafen omfattar varje typ av skada eller kränkning som en behandling i strid med reglerna i personuppgiftslagen, eller föreskrifter som har meddelats av den lagen, har orsakat.

Skälen för bedömningen

Samtliga författningar som berörs av rambeslutet, med undantag av förordningarna om strafförelägganderegister respektive ordningsbotsregister, innehåller hänvisningar som gör 48 § personuppgiftslagen tillämplig på behandling som sker i strid med reg-

lerna i respektive författning. Dessa författningar uppfyller således kraven i rambeslutet.

Frågan är om det beträffande de nyss nämnda registren kan hävdas att bestämmelserna om skadestånd i respektive sektorslag skulle vara tillämplig. En sådan tolkning förefaller tveksam, eftersom skadeståndsreglerna i sektorslagarna tar sikte på behandling i strid med bestämmelser i den lagen. Det är vidare oklart om den allmänna regleringen i polisdatalagen kan anses tillämplig på ordningsbotsregistret. Personuppgiftsbehandling i strafförelägganderegister undantas uttryckligen från regleringen i förordningen om behandling av personuppgifter inom åklagarväsendet.

Det kan inte heller hävdas att statens allmänna skadeståndsansvar enligt skadeståndslagen är tillräckligt. Detta täcker nämligen inte varje form av otillåten behandling av personuppgifter, vilket rambeslutet kräver. När det gäller de båda förordningarna förefaller således kompletterande regler vara nödvändiga.

Här kan också anmärkas att frågan om skadestånd vid kränkning nyligen har utretts. I promemorian Skadeståndsfrågor vid kränkning (Ds 2007:10) föreslås bl.a. ett tillägg i 3 kap. 2 § skadeståndslagen, som innebär att ideellt skadestånd vid myndighetsutövning utgår när någons person, frihet, frid eller ära allvarligt kränkts, oavsett om det föreligger brott. Promemorian har remissbehandlats. Inte heller en sådan ändring torde vara tillräcklig för att uppfylla kraven i rambeslutet.

8.17 Sanktioner

Bedömning: Personuppgiftslagens straffbestämmelse är inte tillämplig på de aktuella författningarna. Det är tveksamt om det, vid sidan av straffansvaret för dataintrång och brott mot tystnadsplikt, finns någon straffbestämmelse som täcker rambeslutets krav på sanktioner för överträdelser. Det kan därför finnas skäl att närmare överväga behovet av straffbestämmelser i det fortsatta arbetet.

Innehållet i rambeslutet

Rambeslutet ställer i *artikel 24* krav på effektiva, proportionella och avskräckande påföljder för överträdelser av bestämmelser som antagits i enlighet med rambeslutet. Det står medlemsstaterna fritt att göra vilka medel som ska användas.

Personuppgiftslagen

Dataskyddsdirektivet förutsätter sanktioner för överträdelser av bestämmelserna i direktivet. Av det skälet infördes en straffbestämmelse i 49 § personuppgiftslagen, som föreskriver straffansvar för överträdelser av olika bestämmelser i personuppgiftslagen. Medan all behandling av personuppgifter i strid med personuppgiftslagen kan ge upphov till skadestånd, är det bara ett fåtal förfaranden som är straffbelagda. Regeringen framhöll att de huvudsakliga sanktionerna är möjligheterna att utdöma skadestånd och använda vite. Dessa sanktioner ansågs i samband med lagens tillkomst som effektiva och i stort sett tillräckliga (prop. 1997/98:44 s. 108).

Viss kriminalisering ansågs dock nödvändig, men den begränsades till några få områden. Den som uppsåtligen eller av grov oaktsamhet lämnar osanna uppgifter i vissa hänseenden, behandlar personuppgifter i strid med bl.a. reglerna om behandling av

känsliga uppgifter, för över uppgifter till tredje land i strid med lagen eller underlåter att göra viss anmälan, döms till böter eller fängelse i sex månader. Om brottet är grovt är straffet fängelse i högst två år.

De i detta ärende aktuella författningarna med särbestämmelser om personuppgiftsbehandling innehåller varken någon hänvisning till 49 § personuppgiftslagen eller några särskilda straffbestämmelser. Detta gäller såväl sektorsförfattningarna som de författningar som reglerar enskilda register.

Frågan är då om personuppgiftslagens straffbestämmelse är tillämplig i de fall där det varken finns någon särskild straffbestämmelse eller någon hänvisning som gör 49 § personuppgiftslagen tillämplig. Lagrådet har i ett tidigare lagstiftningsärende (prop. 2000/01:33 s. 346) ansett att legalitetsprincipen medför att den paragrafen inte kan ges motsvarande tillämpning på bestämmelser som avviker från personuppgiftslagen och som har tagits in i särlagstiftning.

Skälen för bedömningen

Vilka sanktioner kan förekomma?

Inledningsvis bör framhållas att det anses vara en allmän rättsgrundsats att en av de sanktionsformer som utgör skyddet i personuppgiftslagen, nämligen vite, inte bör användas mot statliga myndigheter. Även om 44 § personuppgiftslagen skulle vara tillämplig för en viss myndighets verksamhet torde således vitesanktionen inte kunna användas. Enligt den lagstiftning som gäller för Tullverket har tillsynsmyndigheten inte rätt att förelägga vite. I förslagen till ny lagstiftning för Kustbevakningen (SOU 2006:18 s. 200), polisen (Ds 2007:43 s. 121) och domstolsväsendet (SOU 2000:100 s. 110) föreslås inte heller att tillsynsmyndigheten ska få använda vite.

Det sagda innebär att andra sanktionsformer måste väljas. Skadestånd har behandlats i avsnitt 8.16. Det som då återstår är frågan om straffansvar.

Behövs det en straffbestämmelse?

Det förhållandet att personuppgiftslagen innehåller en straffbestämmelse kan ses som en markering av att lagstiftaren ser kriminalisering som en i sammanhanget viktig åtgärd för att skydda den enskildes integritet. Det bör anmärkas att dataskyddsdirektivet har ett svagare formulerat krav när det gäller sanktioner än rambeslutet.

Straffbestämmelser som i stort sett motsvarar 49 § personuppgiftslagen har också tagits in i 6 kap. 2 § lagen (2007:258) om behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst samt i 6 kap 2 § lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet. Detta motiverades med att bestämmelser om straff fyller en viktig funktion för att markera allvaret i överträdelser till skydd för enskildas integritet (prop. 2006/07:46 s. 106).

Det kan också anmärkas att såväl i den utredning som föregick lagen (1990:90) om behandling av personuppgifter i Skatteverkets brottsbekämpande verksamhet (SOU 1998:9 s. 161) som i propositionen (prop. 1998/99:34 s. 41) argumenterades för behovet av en straffbestämmelse motsvarande 49 § personuppgiftslagen. Lagen kom dock aldrig att innehålla någon sådan.

Vid översynen av personuppgiftsbehandlingen inom domstolsväsendet föreslås också att 49 § personuppgiftslagen skall vara tillämplig (SOU 2000:100 s. 111).

Förslagen till lag om behandling av personuppgifter i polisens brottsbekämpande verksamhet och lag om polisens spaningsregister innehåller däremot, i likhet med den nuvarande polisdatalagen, inte någon straffbestämmelse. Motivet för detta är att behandlingen av personuppgifter ska utföras av personer som är

anställda vid statliga myndigheter och som redan omfattas av bestämmelserna om tjänstefel i brottsbalken (se Ds 2007:43 s. 123). Ställningstagandet bör se mot bakgrund av att regeringen i propositionen om polisens register (prop. 1997/98:97 s. 109) uttalade att när en myndighet inom polisväsendet eller annan myndighet är personuppgiftsansvarig, det inte torde bli aktuellt att tillämpa straffbestämmelsen i personuppgiftslagen och att Polisdatautredningen ansåg att någon straffbestämmelse inte behövdes (SOU 2001:92 s. 193). En motsvarande bedömning gjordes i lagstiftningsärendet om personuppgiftsbehandling i Tullverkets brottsbekämpande verksamhet (prop. 2004/05:164 s. 55).

Inledningsvis bör konstateras att bestämmelsen om tjänstefel är subsidiär till alla andra straffbestämmelser. Frågan är då om de allmänna straffbestämmelserna i brottsbalken uppfyller kravet i rambeslutet. Vad först gäller bestämmelsen om dataintrång i 4 kap. 9 c § brottsbalken får den, med sin breda kriminalisering, anses väl uppfylla kravet vad gäller otillåten behandling i form av ändring, radering, förstörande och liknande åtgärder. Den täcker likaså varje handlande som innebär att någon skaffar sig tillgång till personuppgifter i strid med regelverket.

Straffbestämmelsen om brott mot tystnadsplikt i 20 kap. 3 § brottsbalken fyller också en viktig funktion i sammanhanget, eftersom den straffbelägger såväl oaktsamt som uppsåtligt röjande av uppgifter som någon är skyldig att hemlighålla.

En överträdelse av dataskyddsbestämmelser skulle också kunna aktualisera frågan om tjänstefel. Vissa beteenden som är straffbara enligt 49 § personuppgiftslagen kan dock inte föranleda ansvar för tjänstefel, t.ex. att lämna en osann uppgift till en tillsynsmyndighet, och vissa andra torde också falla utanför den straffbestämmelsens tillämpningsområde. Tillämpningsområdet för tjänstefel begränsas nämligen till myndighetsutövning mot enskild. Behandling av personuppgifter torde endast undantagsvis utgöra myndighetsutövning, men kan däremot ingå som ett led i myndighetsutövning och av det skälet falla under straffbestämmelsen. Exempelvis skulle några typer av otillåten behandling, t.ex. avseende känsliga personuppgifter, eventuellt kunna

vara straffbara som tjänstefel. Då måste emellertid även vägas in att ringa brott har undantagits från det straffbara området för tjänstefel. Bedömningen av om gärningen är ringa ska ske främst mot bakgrund av gärningens betydelse för myndighetsutövningen och gärningsmannens ansvar i förhållande till denna. Det sagda innebär bl.a. att personal som inte har en självständig ställning eller som enbart har biträtt med en begränsad uppgift sällan kan dömas för tjänstefel. Även den skada eller risk för skada som gärningen har vållat ska vägas in vid bedömningen av om gärningen är ringa. Sammanfattningsvis är det osäkert hur långt straffbestämmelsen sträcker sig och i vilken mån den kan uppfylla kraven i rambeslutet.

Däremot torde disciplinärt ansvar eventuellt kunna komma i fråga. Det är dock tveksamt om en sådan sanktion kan betraktas som tillräckligt avskräckande. Härtill kommer att disciplinansvar sällan utkrävs, och dessutom anses vara olämpligt utformat, för förseelser som riktar sig mot tredje man. Disciplinansvaret är nämligen i första hand tänkt att tillämpas vid förseelser riktade mot arbetsgivaren, t.ex. onykterhet i tjänsten.

Det kan således finnas skäl att närmare överväga behovet av en särskild straffbestämmelse för överträdelser av dataskyddsbestämmelser i det fortsatta arbetet. Införandet av en straffbestämmelse skulle kräva ändring inte bara i polisdatalagen och flera andra sektorsförfattningar utan även i författningar som reglerar enskilda register.

8.18 Automatiserade beslut

<p>Bedömning: Det krävs ingen ny lagstiftning om automatiserade beslut nu.</p>

Innehållet i rambeslutet

I *artikel 8* regleras automatiserade beslut. Med detta avses beslut som dels har rättsliga följder för någon eller som annars påverkar honom eller henne negativt, dels enbart grundas på en automatisk behandling avsedd att bedöma vissa personliga egenskaper. Rambeslutet tillåter automatiserade beslut, men endast om dessa har stöd i lag och det i lagen fastställs skyddsåtgärder för den enskilde.

Personuppgiftslagen

I artikel 15 i dataskyddsdirektivet föreskrivs skydd för den registrerade mot vissa automatiserade beslut. Sådana får endast förekomma om de har stöd i lag. Den registrerade tillförsäkras dessutom rätt till viss information. För att uppfylla kraven i dataskyddsdirektivet infördes i en bestämmelse om automatiserade beslut i 29 § personuppgiftslagen (se prop. 1997/98:44 s. 88 f.).

Skälen för bedömningen

Personuppgiftslagen är en sådan lag som anges i rambeslutet och 29 § personuppgiftslagen uppfyller kraven på skyddsåtgärder för den enskilde. Sverige uppfyller således redan kraven i rambeslutet, under förutsättning att det i de författningar som innehåller direkta hänvisningar till personuppgiftslagen görs klart att den bestämmelsen gäller. Det kan noteras att lagen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet inte innehåller någon sådan hänvisning. Skälet för detta torde vara att man inte har sett någon praktiskt behov av en hänvisning, eftersom det inte förekommer några automatiserade beslut i verksamheten. Någon sådan hänvisning har inte heller föreslagits för vare sig polisens framtida behandling av personuppgifter eller för

Kustbevakningens. I båda fallen föreslås lagarna innehålla hänvisningar till de regler i personuppgiftslagen som ska gälla.

Eftersom rambeslutet innehåller regler om information till den registrerade, som delvis avviker från regleringen i 29 § personuppgiftslagen, kan det i framtiden bli nödvändigt att införa särskilda bestämmelser om automatiserade beslut, om polisen eller någon annan brottsbekämpande myndighet vill använda sig av sådana beslut. Det torde däremot inte finnas något omedelbart behov av sådan lagstiftning.

Det kan finnas skäl att här nämna att trafikövervakning med hjälp av hastighetskameror inte uppfyller samtliga rekvisit för automatiserade beslut och således inte berörs. Detta beror på att bilderna från sådana kameror kontrolleras manuellt innan beslut fattas om huruvida den som syns på bilden ska lagföras eller inte.

8.19 Övriga frågor

<p>Bedömning: Övriga delar av rambeslutet kräver inga lagstiftningsåtgärder.</p>

Slutartiklarna

Enligt *artikel 27* påverkar rambeslutet inte sådana avtal som medlemsstaterna eller Europeiska unionen har ingått innan rambeslutet antogs. Vid tillämpningen av sådana avtal ska dock överföring av uppgifter till tredje land eller till internationella organ ske med respekt för bestämmelserna i artikel 14 punkten 1 c och punkten 2 om förhandsmedgivande.

Artikel 27 b reglerar förhållandet till tidigare antagna unionsakter. Om dessa reglerar utbyte av personuppgifter eller tillgång till informationssystem som inrättats enligt fördraget om Europeiska unionen och innehåller särskilda villkor för mottagarens användning av uppgifterna ska sådana villkor ha företräde fram-

för reglerna i rambeslutet. Som exempel kan nämnas Schengens informationssystem.

I *artikel 27 a* föreskrivs att rambeslutet ska utvärderas efter tre år, särskilt med avseende på konsekvenserna av att tillämpningsområdet har begränsats till uppgifter som har överförts eller gjorts tillgängliga.

Rambeslutet ska enligt *artikel 28* genomföras inom två år efter antagandet. Rambeslutet träder i kraft den tjugonde dagen efter det att beslutet har offentliggjorts i Europeiska unionens officiella tidning.

De nu redovisade artiklarna kräver inga lagstiftningsåtgärder.

Utkast till uttalande från rådet

Tillsammans med rambeslutet har presenterats ett utkast till uttalande av rådet, vilket bifogas som *bilaga 2* till denna promemoria. I utkastet uttalas att rådet kommer att undersöka frågan om de uppgifter som fullgörs av de befintliga gemensamma dataskyddsmyndigheter som var för sig har inrättats för Schengens informationssystem, Europol, Eurojust och tullinformationssystemet skulle kunna kombineras inom en enda dataskyddsmyndighet.

Sverige har under förhandlingarna förklarat sig vara positiv till en sådan utveckling.

9 Antagande av rambeslutet

9.1 Godkännande av rambeslutet

Förslag: Sverige ska godkänna det inom Europeiska unionen upprättade utkastet till rambeslut om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete.

Skälen för förslaget

Utökat samarbete ger nya förutsättningar

Både den ökade gränsöverskridande brottsligheten och den större rörligheten för personer skapar behov av ett tätare samarbete mellan de brottsbekämpande myndigheterna i olika länder och utökade möjligheter till rättslig hjälp i brottmål. Europol fyller en viktig funktion i samarbetet mellan brottsbekämpande myndigheter, samtidigt som Eurojust och EJN har fått allt viktigare roller i arbetet med att förbättra det straffrättsliga samarbetet. Under senare år har dessutom en rad olika instrument förhandlats fram inom Europeiska unionen som ger medlemsstaterna större möjligheter att på ett enkelt sätt utbyta information med varandra, att verkställa påföljder beslutade i andra medlemsstater och att arbeta tillsammans med brottsbekämpande uppgifter.

Beträffande samarbetet mellan brottsbekämpande myndigheter kan informationsrambeslutet, Prövrådsbeslutet och VIS-rådsbeslutet nämnas som exempel på den snabba utvecklingen.

Det pågår också ett intensivt arbete med att utveckla det straffrättsliga samarbetet. Efter de redan genomförda rambesluten om en europeisk arresteringsorder och om frysning är ett rambeslut om en europeisk bevisinhämtningsorder nu aktuellt. När det gäller straffverkställighet kan nämnas rambesluten om tillämpning av principen om ömsesidigt erkännande på bötesstraff respektive förverkande, som är de första exemplen på instrument om ömsesidigt erkännande. Nu är ett rambeslut om tillämpning av principen om ömsesidigt erkännande på brottmålsdomar avseende frihetsstraff aktuellt.

Det ökade samarbetet gynnar framför allt effektiviteten i brottsbekämpning och lagföring och skapar betydligt bättre förutsättningar att angripa allvarlig och gränsöverskridande brottslighet. Det är viktigt att den information som finns om allvarliga hot mot samhället kan utnyttjas, oavsett var den finns, och att brottsligheten i största möjliga utsträckning kan hejdas innan den vållar allvarliga problem.

Ökat skydd för personuppgiftsbehandling är nödvändigt

Det ökade informationsflödet har emellertid också nackdelar. Det kan leda till att myndigheterna samlar på sig stora mängder information om enskilda individer. Ett utökat informationsutbyte ställer därför krav på ett gott skydd för den enskildes personliga integritet. Eftersom dataskyddsdirektivet inte omfattar verksamhet på det polisiära och straffrättsliga området utgör dataskyddsrambeslutet en viktig motvikt. Rambeslutet har tillkommit i det uttalade syftet att öka den enskildes skydd mot felaktig eller otillbörlig behandling av personuppgifter vid polisiärt och straffrättsligt samarbete över gränserna.

Antagandet av rambeslutet är en högt prioriterad fråga inom Europeiska unionen, för att nå den önskade balansen mellan å

ena sidan effektiv brottsbekämpning och å andra sidan nödvändigt integritetsskydd.

Det är självfallet viktigt att den enskilde har ett bra skydd mot felaktig behandling av personuppgifter inom detta viktiga område. Sverige har under lång tid varit drivande både i fråga om ett ökat informationsutbyte och i fråga om skydd för den enskildes integritet mot alltför extensiv behandling av personuppgifter. Rambeslutet är ett stort steg framåt i detta avseende. Sverige bör därför medverka till att rambeslutet antas. Bara ett fåtal länder har parlamentariska reservationer mot rambeslutet. Mot den bakgrunden är det angeläget att Sverige snabbt kan lyfta sin parlamentariska reservation, så att rambeslutet kan träda i kraft.

Riksdagens godkännande krävs

Inom ramen för samarbetet inom Europeiska unionens tredje pelare har, till skillnad från samarbetet inom den första pelaren, någon beslutskompetens inte överlåtits till unionen. Innan Sverige röstar för ett antagande av ett rambeslut måste därför, enligt 10 kap. 2 § regeringsformen, riksdagens godkännande inhämtas, om rambeslutet som i detta fall förutsätter lagändringar eller annars bedöms vara av större vikt.

9.2 Skälen för att några lagförslag inte läggs fram

I denna promemoria redovisas innehållet i utkastet till rambeslut och hur rambeslutet förhåller sig till svensk rätt. Promemorian utmynnar i förslag om att Sverige ska godkänna utkastet till rambeslut, men några lagförslag presenteras inte. Däremot lämnas en allmän beskrivning av i vilka avseenden rambeslutet bedöms kräva lagändringar. Avsikten är att lämna förslag till lagändringar efter det att riksdagen – på grundval av en särskild proposition – har godkänt utkastet.

Det är, som riksdagen framhållit vid flera tillfällen, givetvis önskvärt att i samband med att ett utkast till rambeslut läggs fram för riksdagens godkännande även presentera de lagändringar som behövs för att genomföra beslutet. Riksdagen har emellertid ansett att det är möjligt att godkänna ett utkast till råds- eller rambeslut och först därefter fatta beslut om aktuella lagstiftningsåtgärder. Att avvakta med följdlagstiftning på detta sätt bör enligt riksdagens uttalanden emellertid endast ske när det är nödvändigt på grund av de tidsramar som gäller för antagandet av beslutet. Utgångspunkten bör vara att riksdagen, när den beslutar i fråga om godkännande av en överenskommelse, också har möjlighet att ta ställning till de lagändringar som blir aktuella till följd av överenskommelsen.

Beträffande det nu aktuella utkastet till rambeslut har det inom rådet träffats en principöverenskommelse om beslutets innehåll. Sverige kan lyfta sin parlamentariska granskningsreservation först efter det att riksdagens godkännande har inhämtats. Rambeslutet har ett mycket brett tillämpningsområde och berör lagstiftning om behandling av personuppgifter inom såväl polisväsendet som Tullverket, Kustbevakningen, åklagarväsendet, Skatteverket, domstolsväsendet och kriminalvården. Inom flera av dessa områden pågår reformarbete. Polisdatalagen (1998:622), som har en central roll i sammanhanget, är som framgår av avsnitt 6.1 för närvarande under omarbetning. I november 2007 remitterades en promemoria med förslag till lagändringar (Ds 2007:43; Behandling av personuppgifter i polisens brottsbekämpande verksamhet). En ny lag kan förväntas träda i kraft tidigast den 1 januari 2009. Personuppgiftsbehandlingen inom både Kustbevakningen (se avsnitt 6.6) och domstolsväsendet (avsnitt 6.7) har varit föremål för översyn. Betänkandena har remissbehandlats och det pågår nu arbete inom Regeringskansliet i syfte att modernisera regleringen på båda områdena. Vidare har regeringen tillsatt en utredare som ska se över åklagarväsendets behandling av personuppgifter (se avsnitt 6.8). Den utredningen ska presentera sitt arbete under senare delen av år 2008. Dessutom kommer förslag till ny lagstiftning om Schengens informa-

tionssystem att föreläggas riksdagen under år 2008 (se avsnitt 6.2). Vidare kommer genomförandet av Prümrådsbeslutet och VIS-rådsbeslutet att kräva lagändringar inom samma område ungefär samtidigt (se avsnitten 6.3 och 6.4). Till detta kommer att det pågår förhandlingar inom Europeiska unionen dels om flera andra instrument som också berörs av rambeslutets tillämpningsområde, dels om en ny rättslig ram för Europols verksamhet (se avsnitt 7.1). Frågan om ändrade arbetsformer för Eurojust och för European Judicial Network (EJN) också är föremål för diskussion (se avsnitten 7.2 och 7.3). Inom samtliga områden är frågor som rör behandling av personuppgifter ett centralt inslag.

Det pågående reformarbetet både i Sverige och inom Europeiska unionen inom de områden som berörs av rambeslutet innebär att det är nära nog omöjligt att nu ta ställning till vilka lagstiftningsändringar som slutligen kan komma att krävas. I avsnitt 8 har emellertid redovisats vilka lagändringar som rambeslutet kan väntas föranleda.

Om Sverige skulle avvakta med att godkänna utkastet till rambeslut till dess att det finns ett tillfredsställande beredningsunderlag i fråga om behovet av lagändringar och den närmare utformningen av dessa, skulle det innebära en avsevärd försening av antagandet av rambeslutet. En sådan fördröjning kan ibland accepteras, men vore i detta fall särskilt olycklig eftersom rambeslutet dels syftar till att stärka enskildas rättigheter vid personuppgiftsbehandling dels har stor betydelse för utvecklingen av andra instrument. Mot den bakgrunden finns det i detta fall starka skäl för regeringen att föreslå riksdagen att godkänna utkastet till rambeslut utan att regeringen samtidigt lägger fram de förslag till lagändringar som bedöms vara nödvändiga.

10 Ekonomiska konsekvenser

Vid översyner av personuppgiftsbehandlingen inom polisen, tullväsendet, Kustbevakningen, domstolarna och kriminalvården har genomgående gjorts bedömningen att det inte uppstår några mer påtagliga kostnadsökningar. De lagstiftningsåtgärder som kan komma att aktualiseras vid genomförande av rambeslutet är till stor del av det slaget att de inte medför några kostnader. Som framgått rör det sig om betydligt färre och mindre ingripande ändringar än när personuppgiftslagen infördes, vilket inte ansågs motivera några anslagsökningar. I detta fall ska dessutom eventuellt ökade kostnader för ändringar i befintliga system vägas mot de förbättringar och effektiviseringar som ett ökat informationsutbyte och ett förbättrat straffrättsligt samarbete innebär. Mot den bakgrunden görs bedömningen att eventuella extrakostnader som uppkommer bör rymmas inom befintlig budgetram.

Utkastet till rambeslut om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete



**EUROPEISKA
UNIONENS RÅD**

**Bryssel den 11 december 2007 (17.12)
(OR. en)**

16069/07

**Interinstitutionellt ärende:
2005/0202 (CNS)**

LIMITE

**CRIMORG 184
DROIPEN 117
ENFOPOL 210
DATAPROTECT 58
ENFOCUSTOM 122
COMIX 1040**

LÄGESRAPPORT

från: RIF-råden
av den: 30 november 2007

Föreg. dok. nr: 14119/1/07 REV 1 CRIMORG 153 DROIPEN 94 ENFOPOL 170
DATAPROTECT 47 ENFOCUSTOM 102 COMIX 901

Ärende: Förslag till rådets rambeslut om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete

1. Den 4 oktober 2005 översände kommissionen ett förslag till rådets rambeslut om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete ("rambeslutet") till rådets generalsekretariat. Den 13 december 2005 bad rådet Europaparlamentet att yttra sig om förslaget. Europaparlamentet avgav sitt yttrande den 27 september 2006. Sedan dess har Europaparlamentet, den 6 juni 2007, avgivit ett andra yttrande över det reviderade utkastet.

2. Vid mötet mellan den gemensamma kommittén på ministernivå och rådet den 8–9 november 2007 nådde man fram till en allmän riktlinje om utkastet till rambeslut, med förbehåll för ytterligare omarbetning av ingressen och förbättring av bestämmelsernas rättsliga kvalitet. Vid RIF-rådets möte den 30 november 2007 tillstyrkte delegationerna de ändringar i ingressen och artikel 1 som anges i bilaga I.
DK, IE, NL, SE och UK har reservationer för parlamentsbehandling.

3. När Europaparlamentet har hörts på nytt kommer utkastet till rambeslut att granskas av juristlingvisterna.

RÅDETS RAMBESLUT

av den ...

om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete

EUROPEISKA UNIONENS RÅD HAR ANTAGIT DETTA BESLUT

med beaktande av fördraget om Europeiska unionen, särskilt artiklarna 30, 31 och 34.2 b,

med beaktande av kommissionens förslag¹,

med beaktande av Europaparlamentets yttrande², och

av följande skäl:

- (1) Europeiska unionen har som mål att bevara och utveckla unionen som ett område med frihet, säkerhet och rättvisa. En hög säkerhetsnivå ska uppnås genom gemensamma insatser från medlemsstaternas sida när det gäller polissamarbete och straffrättsligt samarbete.
- (2) Gemensamma insatser på polissamarbetets område i enlighet med artikel 30.1 b i fördraget om Europeiska unionen och gemensamma insatser rörande straffrättsligt samarbete i enlighet med artikel 31.1 a i samma fördrag innebär att det blir nödvändigt att behandla relevanta uppgifter, vilket bör omfattas av lämpliga bestämmelser om skydd av personuppgifter.

1

2 ...

...

- (3) Lagstiftning som omfattas av avdelning VI i fördraget om Europeiska unionen syftar till att främja polissamarbete och rättsligt samarbete med avseende på såväl samarbetets effektivitet som dess överensstämmelse med lagen och med grundläggande rättigheter, särskilt rätten till ett privatliv och rätten till skydd av personuppgifter. Gemensamma normer för behandling och skydd av personuppgifter i syfte att förebygga och bekämpa brott kan bidra till att uppnå dessa båda mål.
- (4) I Haagprogrammet för stärkt frihet, säkerhet och rättvisa i Europeiska unionen, som antogs av Europeiska rådet den 4 november 2004, understryks behovet av en innovativ strategi i fråga om gränsöverskridande utbyte av information om brottsbekämpning, under noggrant iakttagande av centrala villkor på området skydd av personuppgifter. Kommissionen uppmanades att senast i slutet av 2005 lägga fram förslag om detta. Detta återspeglas i *rådets och kommissionens handlingsplan för genomförande av Haagprogrammet för ett stärkt område med frihet, säkerhet och rättvisa*³.
- (5) Utbytet av personuppgifter inom ramen för polissamarbetet och det straffrättsliga samarbetet, särskilt enligt den princip om tillgänglighet som tas upp i Haagprogrammet, bör bygga på klara (...) regler som stärker det ömsesidiga förtroendet mellan behöriga myndigheter och garanterar att den relevanta informationen skyddas på ett sätt som utesluter all diskriminering mot samarbetet mellan medlemsstaterna samtidigt som enskildas grundläggande rättigheter respekteras fullt ut. Befintliga instrument på europeisk nivå är inte tillräckliga. 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 uppgifter⁴ är inte tillämpligt i fråga om behandling av personuppgifter i samband med verksamheter som faller utanför gemenskapsrättens tillämpningsområde, till exempel sådana som anges i avdelning VI i fördraget om Europeiska unionen, och under inga omständigheter på uppgiftsbehandling som rör allmän säkerhet, försvar, nationell säkerhet och statlig verksamhet på det straffrättsliga området.

³ EUT C 198, 12.8.2005, s. 1.

⁴ EGT L 281, 23.11.1995, s. 31.

- (5a) Rambeslutet är endast tillämpligt på uppgifter som de behöriga myndigheterna samlar in eller behandlar för att kunna förebygga, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder. I rambeslutet överläts det till medlemsstaterna att på nationell nivå mer exakt besluta vilka andra ändamål som ska anses förenliga med det ändamål för vilket personuppgifterna ursprungligen insamlades. I allmänhet är ytterligare behandling för historiska, statistiska eller vetenskapliga ändamål inte förenliga med det ursprungliga ändamålet för behandlingen.
- (6) Rambeslutets tillämpningsområde begränsas till behandlingen av sådana personuppgifter som överförs eller görs tillgängliga mellan medlemsstaterna. Inga slutsatser kan dras av denna begränsning beträffande Europeiska unionens behörighet att anta rättsakter om insamling och behandling av personuppgifter på nationell nivå eller det lämpliga i att unionen gör detta i framtiden.
- (6a) I syfte att underlätta informationsutbytet inom Europeiska unionen vill medlemsstaterna säkerställa att den standard i fråga om dataskydd som fastställs inom nationell databehandling ska motsvara den som föreskrivs i rambeslutet. När det gäller nationell databehandling hindrar detta rambeslut inte medlemsstaterna från att föreskriva garantier för skydd av personuppgifter högre än dem som fastställs i detta rambeslut.
- (6b) Detta rambeslut ska inte tillämpas på personuppgifter som en medlemsstat erhållit inom tillämpningsområdet för detta rambeslut och som härrör från denna medlemsstat.
- (7) Tillnärmningen av medlemsstaternas lagstiftningar bör inte leda till några försämringar i det dataskydd de ger utan i stället syfta till att garantera en hög skyddsnivå inom unionen.

- (8) Det är nödvändigt att precisera målen med skyddet av personuppgifter inom ramen för polisens och domstolarnas verksamheter och att införa bestämmelser om vilken behandling av personuppgifter som är tillåten i syfte att säkerställa att uppgifter som kan komma att utbytas har behandlats på lagligt sätt och i enlighet med grundläggande principer i fråga om uppgifters kvalitet. Samtidigt är det viktigt att inte polisens, tullens, domstolarnas eller andra behöriga myndigheters legitima verksamheter sätts på spel.
- (8a) Principen om uppgifters korrekthet ska tillämpas med beaktande av den aktuella behandlingens art och syfte. Så grundar sig exempelvis uppgifterna inom framför allt rättsliga förfaranden på enskilda personers subjektiva uppfattning och kan i vissa fall omöjliga kontrolleras. Följaktligen kan inte korrekthetskravet röra korrektheten i ett uttalande utan blott och bart det faktum att ett visst uttalande har gjorts. (...)
- (8b) Arkivering i ett separat dataset ska tillåtas endast om uppgifterna inte längre krävs eller används för förebyggande, utredning, avslöjande eller lagföring av brott eller verkställighet av straffrättsliga påföljder. Arkivering i ett separat dataset ska även tillåtas om de arkiverade uppgifterna lagras i en databas tillsammans med andra uppgifter på ett sådant sätt att de inte längre kan användas för förebyggande, utredning, avslöjande eller lagföring av brott eller verkställighet av straffrättsliga påföljder. Lämplig längd av arkiveringsperioden är avhängig av syftet med arkiveringen och de registrerade personernas legitima intressen. I fråga om arkivering för historiska ändamål kan man också fastställa en mycket lång period.
- (8c) Uppgifter får också utgå genom att datamediet förstörs.
- (8d) När det gäller icke korrekt, ofullständiga eller inte längre aktuella uppgifter som överförs eller görs tillgängliga för andra medlemmar och behandlas ytterligare av domstolsliknande myndigheter, med vilket avses myndigheter med behörighet att fatta rättsligen bindande beslut, ska rättelse, strykning eller blockerande verkställas enligt nationell lag.

- (9) För att kunna garantera en hög skyddsnivå för personuppgifter om enskilda personer krävs det gemensamma bestämmelser för att fastställa om de uppgifter som behandlas av behöriga myndigheter i medlemsstaterna uppfyller laglighets- och kvalitetskraven.
- (10) Därför bör man på europeisk nivå fastställa de villkor som ska vara uppfyllda för att medlemsstaternas behöriga myndigheter ska ha rätt att till myndigheter och privata parter i medlemsstater överföra och ge tillgång till personuppgifter som erhållits från andra medlemsstater. I många fall är överföring av personuppgifter från domstolsväsendet, polisen eller tullen till privata parter nödvändig för att lagföra brott eller för att avvärja en direkt och allvarlig fara för allmän säkerhet och förhindra att enskilda personers rättigheter lider allvarlig skada, till exempel genom att utfärda varningar avseende förfalskningar av värdepapper till banker och kreditinstitut eller, i fråga om fordonsstölder, genom att överföra personuppgifter till försäkringsbolag för att förhindra olaglig handel med stulna motorfordon eller för att förbättra villkoren för återförande av stulna motorfordon från utlandet. Detta innebär inte överföring av arbetsuppgifter från polis och domstolar till privata parter.
- (10a) Reglerna i detta rambeslut avseende överföring av personuppgifter från domstolsväsendet, polisen eller tullen till privata parter berörs inte av utlämnandet av uppgifter till privata parter (såsom försvarsadvokater och brottsoffer) i samband med brottmål.
- (11) Den vidare behandlingen av personuppgifter som erhållits från eller gjorts tillgängliga av den behöriga myndigheten i en annan medlemsstat, särskilt det att vidarebefordra sådana uppgifter eller göra dem tillgängliga på nytt, bör omfattas av gemensamma bestämmelser på europeisk nivå.
- (11a) När personuppgifter får behandlas ytterligare efter det att den medlemsstat från vilken uppgifterna erhållits har givit sitt samtycke får varje medlemsstat fastställa villkoren för sådant samtycke, inbegripet exempelvis allmänt samtycke för kategorier av information och kategorier av ytterligare behandling.
- (11b) När personuppgifter får behandlas ytterligare för administrativa förfaranden inbegriper dessa förfaranden också åtgärder av (...) reglerings- och kontrollorgan (...).

(11c) Polisens, tullens, domstolarnas eller andra behöriga myndigheters legitima verksamheter kan kräva att uppgifter sänds till myndigheter i tredjestater eller internationella organisationer som har skyldigheter i fråga om att förebygga, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder.

(12) Om uppgifter överförs från en medlemsstat i Europeiska unionen till tredjestater eller internationella organ ska de i princip omfattas av ett adekvat skydd.

(12a) Om personuppgifter överförs från en medlemsstat i Europeiska unionen till tredjeländer eller internationella organ kan en sådan överföring i princip ske endast efter det att den medlemsstat som har lämnat uppgifterna har gett sitt samtycke till överföringen. Varje medlemsstat får bestämma villkoren för ett sådant samtycke, till exempel genom ett generellt samtycke för kategorier av uppgifter eller för vissa angivna länder.

(12b) För ett effektivt samarbete i fråga om brottsbekämpning krävs att om hotet mot en medlemsstats eller en tredjestats allmänna säkerhet är så överhängande att det är omöjligt att i tid inhämta ett förhandsmedgivande kan den behöriga myndigheten överlämna de relevanta personuppgifterna till den berörda tredjestaten utan sådant förhandsmedgivande. Detsamma kan gälla om andra väsentliga, lika betydelsefulla, intressen i en medlemsstat står på spel, exempelvis om en medlemsstats kritiska infrastruktur kan bli föremål för ett överhängande hot eller om en medlemsstats finansiella system kan drabbas av allvarliga störningar.

(13) För att tillförsäkra den registrerade personen ett effektivt rättsskydd kan det bli nödvändigt att informera denne om behandlingen av dennes personuppgifter, särskilt vid synnerligen allvarlig kränkning av dennes rättigheter som ett resultat av hemlig insamling av uppgifter.

- (13a) Medlemsstaterna bör se till att den registrerade personen informeras om att personuppgifter kan eller håller på att samlas in, behandlas eller överföras till en annan medlemsstat för att förebygga, utreda, avslöja och lagföra brott eller verkställa straffrättsliga påföljder. Formerna för den registrerade personens rätt att bli informerad och undantag från denna rätt ska fastställas i den nationella lagstiftningen. Detta kan genomföras på ett generellt sätt, t.ex. genom lagstiftning eller offentliggörande av en förteckning över olika typer av uppgiftsbehandling.
- (14) För att kunna garantera skyddet av personuppgifter utan att äventyra ändamålet med brottsutredningar måste man fastställa den registrerades rättigheter.
- (14a) Några medlemsstater har gett den berörda personen rätt till tillgång till uppgifter i brottmål genom ett system där det nationella kontrollorganet, i den berörda personens ställe, utan någon restriktion har tillgång till alla personuppgifter som rör den berörda personen och även får rätta, stryka eller uppdatera icke korrekta uppgifter. I sådana fall med indirekt tillgång får det i den nationella lagstiftningen i dessa medlemsstater föreskrivas att det nationella kontrollorganet endast kommer att informera den berörda personen om att alla nödvändiga kontroller har utförts. Dessa medlemsstater tillhandahåller emellertid i särskilda fall även möjligheter till direkt tillgång för den berörda personen, såsom tillgång till rättsliga register för att erhålla kopior av egna kriminalregister eller förhör hos polismyndigheterna.
- (15) Det bör införas gemensamma bestämmelser om konfidentiell och säker uppgiftsbehandling, om ansvarsskyldighet och påföljder när uppgifterna används på otillåtet sätt av de behöriga myndigheterna samt om möjligheter för den registrerade till rättslig prövning. Det ankommer dock på varje medlemsstat att själv fastställa utformningen av bestämmelserna om skadeståndsgrundande överträdelser och om vilka påföljder som ska tillämpas vid överträdelse av de nationella dataskyddsbestämmelserna.
- (15a) Detta rambeslut gör att principen om allmänhetens tillgång till offentliga handlingar kan tillgodoses vid tillämpningen av principerna i detta.

- (15b) När så behövs för att skydda personuppgifter med avseende på behandling som genom sin omfattning eller typ innebär särskilda risker för grundläggande rättigheter och friheter, till exempel behandling med ny teknik, nya mekanismer eller förfaranden, bör man säkerställa att den behöriga nationella myndigheten rådfrågas före upprättandet av register för behandling av dessa uppgifter.
- (16) Inrättandet i medlemsstaterna av tillsynsmyndigheter, som fullständigt oberoende genomför sina åligganden, är en mycket viktig del av skyddet av sådana personuppgifter som behandlas inom ramen för polissamarbetet och det straffrättsliga samarbetet mellan medlemsstaterna.
- (16a) Den myndighet som redan inrättats i medlemsstaterna i enlighet med artikel 28 i direktiv 95/46/EG kan också axla ansvaret för de uppgifter som ska utföras av de nationella tillsynsmyndigheter som ska inrättas i enlighet med detta rambeslut.
- (17) Dessa myndigheter bör ha nödvändiga resurser för att kunna genomföra sina uppgifter, inklusive befogenhet att – särskilt när det gäller klagomål från enskilda personer – undersöka och intervensera eller befogenhet att inleda rättsliga förfaranden. De bör även bidra till att sörja för insyn i behandlingen av uppgifter i sina respektive medlemsstater. Emellertid bör deras befogenheter inte inkräkta på särskilda regler som fastställts för brottmål eller på domstolsväsendets oberoende (...).
- (18)

(19) I artikel 47 i fördraget om Europeiska unionen föreskrivs det att ingen bestämmelse i det fördraget ska inverka på fördragen om upprättandet av Europeiska gemenskaperna eller på senare fördrag och rättsakter om ändring eller komplettering av dessa. Följaktligen påverkar detta rambeslut inte skyddet av personuppgifter enligt gemenskapsrätten, särskilt inte det skydd som föreskrivs i Europaparlamentets och rådets direktiv 95/46/EG om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter, Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter⁵ och Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation)⁶.

(20)

(21)

(21a) (...).

(22)

(23) Detta rambeslut påverkar inte bestämmelserna om sådan olaglig tillgång till uppgifter som avses i rådets rambeslut 2005/222/RIF av den 24 februari 2005 om angrepp mot informationssystem⁷.

(24) Detta rambeslut påverkar inte medlemsstaternas eller Europeiska unionens gällande skyldigheter och åtaganden enligt bilaterala och/eller multilaterala avtal med tredjestater. Framtida avtal måste följa bestämmelserna om utbyte med tredjestater.

⁵ EGT L 8, 12.1.2001, s. 1.

⁶ EGT L 201, 31.7.2002, s. 37.

⁷ EUT L 69, 16.3.2005, s. 67.

(24a) Flera rättsakter som antagits på grundval av avdelning VI i EU-fördraget innehåller särskilda bestämmelser om skydd av personuppgifter som överförs eller på något annat sätt behandlas i enlighet med de rättsakterna. I några fall utgör dessa bestämmelser en komplett och enhetlig uppsättning regler som omfattar alla relevanta aspekter av dataskydd (principer om uppgifternas kvalitet, regler om uppgifternas säkerhet, reglering av de registrerades rättigheter och skydd, organisation av kontroll och ansvar) och i dessa regleras frågor mer detaljerat än i rambeslutet. Den relevanta uppsättningen dataskyddsbestämmelser i dessa rättsakter, särskilt de som reglerar funktionssättet för Europol, Eurojust, SIS och tullinformationssystemet (TIS) samt de rättsakter genom vilka medlemsstaternas myndigheter ges direkt tillgång till vissa datasystem i andra medlemsstater, påverkas inte av detta rambeslut. Detsamma gäller de dataskyddsbestämmelser som reglerar automatisk överföring av DNA-profiler, fingeravtrycksuppgifter och uppgifter ur nationella fordonsregister i enlighet med rådets beslut om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet.

(24b) I andra fall är räckvidden för dataskyddsbestämmelser i rättsakter som antagits i enlighet med avdelning VI i EU-fördraget mer begränsade. Ofta fastställs det i dessa rättsakter särskilda villkor för den medlemsstat som från en annan medlemsstat tar emot information innehållande personuppgifter i fråga om de ändamål för vilka den kan använda uppgifterna, medan det i fråga om övriga dataskyddsaspekter hänvisas till Europarådets konvention om skydd för enskilda vid automatisk databehandling av personuppgifter av den 28 januari 1981 eller till nationell lagstiftning.

I den mån det i bestämmelserna i dessa rättsakter fastställs villkor för mottagande medlemsstater för användning eller vidare överföring av personuppgifter vilka är strängare än villkoren i motsvarande bestämmelser i detta rambeslut, ska dessa förstnämnda inte heller påverkas. I alla övriga avseenden ska de regler som fastställs i detta rambeslut gälla.

(25) Detta rambeslut påverkar inte Europarådets konvention av den 28 januari 1981 om skydd för enskilda vid automatisk databehandling av personuppgifter eller tilläggsprotokollet av den 8 november 2001 till denna konvention eller Europarådets konventioner om straffrättsligt samarbete.

- (26) Eftersom målen för den föreslagna åtgärden, nämligen att fastställa gemensamma bestämmelser om skydd av personuppgifter som behandlas inom ramen för polissamarbetet och det straffrättsliga samarbetet, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna och därför, på grund av åtgärdens omfattning och verkningar, bättre kan uppnås på EU nivå, kan rådet vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i EG fördraget, till vilken det hänvisas i artikel 2 i EU fördraget. I enlighet med proportionalitetsprincipen i artikel 5 i EG fördraget går detta rambeslut inte utöver vad som är nödvändigt för att uppnå dessa mål.
- (27) Förenade kungariket deltar i detta rambeslut i enlighet med artikel 5 i protokollet om införlivande av Schengenregelverket inom Europeiska unionens ramar, fogat till fördraget om Europeiska unionen och fördraget om upprättandet av Europeiska gemenskapen, och i enlighet med artikel 8.2 i rådets beslut 2000/365/EG av den 29 maj 2000 om en begäran från Förenade konungariket Storbritannien och Nordirland om att få delta i vissa bestämmelser i Schengenregelverket⁸.
- (28) Irland deltar i detta rambeslut i enlighet med artikel 5 i protokollet om införlivande av Schengenregelverket inom Europeiska unionens ramar, fogat till fördraget om Europeiska unionen och fördraget om upprättandet av Europeiska gemenskapen, och i enlighet med artikel 6.2 i rådets beslut 2002/192/EG av den 28 februari 2002 om Irlands begäran om att få delta i vissa bestämmelser i Schengenregelverket.
- (29) När det gäller Island och Norge utgör detta rambeslut, i enlighet med avtalet mellan Europeiska unionens råd och Republiken Island och Konungariket Norge om dessa staters associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket, en utveckling av bestämmelser i Schengenregelverket vilka rör det område som avses i artikel 1.H och 1.I i rådets beslut 1999/437/EG av den 17 maj 1999 om vissa tillämpningsföreskrifter för det avtalet⁹.

⁸ EGT L 131, 1.6.2000, s. 43.

⁹ EGT L 176, 10.7.1999, s. 31.

- (30) När det gäller Schweiz utgör detta rambeslut, i enlighet med avtalet mellan Europeiska unionen, Europeiska gemenskapen och Schweiziska edsförbundet om Schweiziska edsförbundets associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket, en utveckling av de bestämmelser i Schengenregelverket vilka rör det område som avses i artikel 1.H och 1.I i rådets beslut 1999/437/EG av den 17 maj 1999 jämförd med artikel 4.1 i rådets beslut 2004/849/EG om undertecknande på Europeiska unionens vägnar och provisorisk tillämpning av vissa bestämmelser av det avtalet¹⁰.
- (31)
- (32) Detta rambeslut står i överensstämmelse med de grundläggande rättigheter och principer som erkänns framför allt i Europeiska unionens stadga om de grundläggande rättigheterna. Detta rambeslut syftar till att garantera full respekt för rätten till det skydd för privatlivet och det skydd av personuppgifter som kommer till uttryck i artiklarna 7 och 8 i Europeiska unionens stadga om de grundläggande rättigheterna.

¹⁰ EUT L 368, 15.12.2004, s. 26.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Syfte och tillämpningsområde

1. Syftet med detta rambeslut är att säkerställa en hög skyddsnivå för fysiska personers grundläggande fri- och rättigheter, särskilt när det gäller deras rätt till (...) privatliv, med avseende på behandling av personuppgifter inom ramen för polissamarbete och straffrättsligt samarbete enligt avdelning VI i fördraget om Europeiska unionen och samtidigt garantera en allmän säkerhet på hög nivå.
2. I enlighet med detta rambeslut ska medlemsstaterna skydda fysiska personers grundläggande fri- och rättigheter, och särskilt deras rätt till privatliv (...), när personuppgifter för att förebygga, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder
 - a) förmedlas, har förmedlats, görs eller har gjorts tillgängliga mellan medlemsstaterna,
 - b) förmedlas, har förmedlats, görs eller har gjorts tillgängliga av medlemsstaterna till myndigheter eller informationssystem som inrättats i enlighet med avdelning VI i fördraget om Europeiska unionen, eller
 - c) förmedlas, har förmedlats, görs eller har gjorts tillgängliga för medlemsstaternas behöriga myndigheter av myndigheter eller informationssystem som inrättats i enlighet med fördraget om Europeiska unionen eller fördraget om upprättandet av Europeiska gemenskapen.
3. Detta rambeslut gäller för sådan behandling av personuppgifter som helt eller delvis utförs automatiskt samt för annan behandling än automatisk av sådana personuppgifter som ingår i eller kommer att ingå i ett register.
4. Detta rambeslut påverkar inte viktiga nationella säkerhetsintressen och särskild underrättelseverksamhet inom området nationell säkerhet.

5. Detta rambeslut får inte hindra medlemsstaterna från att föreskriva strängare säkerhetsåtgärder för skydd av personuppgifter som behandlas eller samlas in på nationell nivå än de som fastställs i detta rambeslut.

Artikel 2
Definitioner

I detta rambeslut gäller följande definitioner:

- a) *personuppgifter*: varje upplysning som avser en identifierad eller identifierbar fysisk person (den registrerade). En identifierbar person är en person som kan identifieras, direkt eller indirekt, framför allt genom hänvisning till ett identifieringsnummer eller till en eller flera faktorer som är specifika för hans fysiska, fysiologiska, psykiska, ekonomiska, kulturella eller sociala identitet.
- b) *behandling av personuppgifter (behandling)*: varje åtgärd eller serie av åtgärder som vidtas med personuppgifter, vare sig det sker på automatisk väg eller inte, till exempel insamling, registrering, organisering, lagring, bearbetning eller ändring, hämtning, läsning, användning, utlämnande genom översändande, spridning eller annat tillhandahållande av uppgifter, sammanställning eller samkörning, blockering, radering eller förstöring.
- c) *blockering*: markering av lagrade personuppgifter med syftet att begränsa behandlingen av dessa i framtiden.
- d) *register med personuppgifter (register)*: varje strukturerad samling av personuppgifter som är tillgänglig enligt särskilda kriterier, oavsett om samlingen är centraliserad, decentraliserad eller spridd på grundval av funktionella eller geografiska förhållanden.
- e) *registerförare*: varje organ som behandlar personuppgifter för den registeransvariges räkning.
- f) *mottagare*: varje organ till vilken uppgifterna utlämnas.
- g) *den registrerades samtycke*: varje slag av frivillig, särskild och informerad viljeyttring genom vilken den registrerade godtar behandling av personuppgifter som rör honom.

- h)
- i)
- i) *behöriga myndigheter*: myndigheter som inrättats genom rättsakter antagna av rådet enligt avdelning VI i fördraget om Europeiska unionen, samt polis, tull, domstolar eller andra behöriga myndigheter i medlemsstaterna som genom nationell lag är bemyndigade att behandla personuppgifter inom tillämpningsområdet för detta rambeslut.
- j) *registeransvarig*: en fysisk eller en juridisk person, en myndighet, en avdelning eller varje annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter.
- k) *markering*: markering av lagrade personuppgifter utan syftet att begränsa behandlingen av dessa i framtiden.
- l) *avidentifiering*: att ändra personuppgifter på ett sådant sätt att detaljerna beträffande personliga eller sakliga förhållanden inte längre eller endast med oproportionerligt stor insats i fråga om tid, kostnader och arbete kan tillskrivas en identifierad eller identifierbar fysisk person.

Artikel 3

Principerna om lagenlighet, proportionalitet och ändamål

1. De behöriga myndigheterna får inom ramen för sina uppgifter endast samla in personuppgifter för särskilda, uttryckligt angivna och berättigade ändamål och uppgifterna får endast behandlas för det ändamål som låg till grund för insamlingen av dem. Behandlingen av uppgifterna måste vara befogad, adekvat och relevant.
2. Vidare behandling för ett annat ändamål är tillåten om
 - a) denna vidare behandling inte är oförenlig med det ändamål för vilket uppgifterna samlades in,
 - b) de behöriga myndigheterna i enlighet med tillämpliga rättsliga bestämmelser är bemyndigade att behandla sådana uppgifter, och

- c) denna behandling är nödvändig och står i proportion till det ändamålet.

Dessutom får de översända personuppgifterna behandlas vidare av den behöriga myndigheten för historiska, statistiska eller vetenskapliga ändamål, under förutsättning att medlemsstaterna föreskriver lämpliga säkerhetsåtgärder, som aidentifiering av uppgifterna.

Artikel 4

Rättelse, radering och blockering

1. Personuppgifter ska rättas om de är felaktiga samt, om så är möjligt och nödvändigt, kompletteras eller aktualiseras.
2. Personuppgifter ska raderas eller aidentifieras när dessa inte längre behövs för de ändamål för vilka de lagligen insamlades eller lagligen vidare bearbetas. Arkivering av de uppgifter som införts i en separat databas under en lämplig period i överensstämmelse med national lagstiftning ska inte påverkas av denna bestämmelse.
3. Personuppgifter ska inte raderas utan blockeras, om det finns skälig grund att anta att en radering skulle kunna påverka den registrerades legitima intressen. Blockerade uppgifter får endast behandlas för det ändamål som hindrade att de raderades.
4. Om personuppgifterna ingår i ett domstolsbeslut eller register i samband med utfärdandet av ett rättsligt beslut ska rättelse, radering eller blockering utföras i enlighet med nationella bestämmelser om rättsliga förfaranden.

Artikel 5

Artikel 6

Fastställande av tidsfrister för radering och kontroll

För radering av personuppgifter eller en regelbunden kontroll av nödvändigheten av lagringen ska lämpliga tidsfrister fastställas. Genom föreskrifter om förfarandena ska det garanteras att tidsfristerna efterlevs.

Artikel 7

Behandling av särskilda kategorier av uppgifter

Behandling av personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening samt uppgifter som rör hälsa och sexualliv får endast förekomma när detta är absolut nödvändigt och om det i den nationella lagstiftningen tillhandahålls tillräckliga skyddsåtgärder.

Artikel 8

Datoriserade beslut

Ett beslut som har negativa rättsliga följder för den registrerade eller som väsentligt berör honom eller henne och som enbart grundas på en automatisk behandling avsedd att bedöma vissa personliga egenskaper ska endast vara tillåtet om detta är stadgat i en lag där det fastställs skyddsåtgärder för den registrerades legitima intressen.

Artikel 9

Kontroll av kvaliteten på de uppgifter som översänds eller görs tillgängliga

1. De behöriga myndigheterna ska vidta alla rimliga åtgärder för att se till att personuppgifter som är felaktiga, ofullständiga eller inte längre uppdaterade inte översänds eller görs tillgängliga. De behöriga myndigheterna ska därför i görligaste mån kontrollera kvaliteten på personuppgifterna innan dessa översänds eller görs tillgängliga. Vid all översändning av uppgifter ska, så långt detta är möjligt, sådan tillgänglig information läggas till som gör att den mottagande medlemsstaten kan bedöma graden av korrekthet, fullständighet, aktualitet och tillförlitlighet. Om personuppgifter översänds utan att någon begäran har gjorts ska den mottagande myndigheten utan dröjsmål bedöma huruvida dessa uppgifter är nödvändiga för det ändamål som låg till grund för översändningen.

2. Om det visar sig att felaktiga uppgifter har översänts eller att uppgifter olovligen har översänts ska mottagaren omedelbart underrättas om detta. Uppgifterna måste ofördröjligen rättas, raderas eller blockeras i enlighet med artikel 4.

Artikel 10

Tidsfrister

1. Den översändande myndigheten får när den översänder uppgifter eller gör dessa tillgängliga enligt nationell lagstiftning och enligt artiklarna 4 och 6 meddela de tidsfrister för lagring av uppgifterna efter vilka även mottagaren ska radera eller blockera uppgifterna eller kontrollera om dessa fortfarande behövs. Denna skyldighet ska inte tillämpas, om dessa uppgifter vid utgången av tidsfristerna krävs för en pågående utredning, lagföring av brott eller verkställighet av straffrättsliga påföljder.
2. Om den översändande myndigheten inte har angivit en tidsfrist enligt punkt 1 ska tidsfristerna enligt artiklarna 4 och 6 för lagring av uppgifterna enligt de mottagande medlemsstaternas nationella lagstiftning tillämpas.

Artikel 11

Registrering och dokumentation

1. Varje överföring av personuppgifter ska registreras eller dokumenteras för att man ska kunna kontrollera om behandlingen av uppgifterna är lagenlig, utföra egenkontroll samt garantera integritet och säkerhet för uppgifterna.
2. Registrering och dokumentation utformad enligt punkt 1 ska översändas till den för skydd av uppgifter behöriga tillsynsmyndigheten, om denna så begär. Den behöriga tillsynsmyndigheten får använda dessa uppgifter endast för att kontrollera skyddet av personuppgifter, för att garantera att behandlingen fungerar tillfredsställande och för att sörja för uppgifternas integritet och säker uppgiftsbehandling.

Artikel 12

Behandling av personuppgifter som översänts från eller gjorts tillgängliga av en annan medlemsstat

1. Personuppgifter som översänts från eller gjorts tillgängliga av den behöriga myndigheten i en annan medlemsstat får, i enlighet med kraven i artikel 3.2, endast bearbetas vidare för följande ändamål, utöver dem för vilka de översändes eller gjordes tillgängliga:
 - a) För att förebygga, utreda, avslöja eller lagföra brott eller för att verkställa straffrättsliga påföljder, varvid det inte rör sig om samma brott eller påföljder för vilka uppgifterna översändes eller gjordes tillgängliga.
 - b) För andra rättsliga eller administrativa förfaranden med direkt anknytning till förebyggande, utredning, avslöjande eller lagföring av brott eller verkställighet av straffrättsliga påföljder.
 - c) För att avvärja en direkt och allvarlig fara för den allmänna säkerheten.
 - d) För varje annat syfte endast med förhandsmedgivande från den översändande medlemsstaten eller med den registrerades samtycke givet i överensstämmelse med nationell lagstiftning.

Dessutom får de översända personuppgifterna behandlas vidare av den behöriga myndigheten för historiska, statistiska eller vetenskapliga ändamål under förutsättning att medlemsstaterna föreskriver lämpliga säkerhetsåtgärder som avidentifiering av uppgifterna.

Artikel 13

Iakttagande av nationella restriktioner för behandling av uppgifter

1. Om särskilda restriktioner för behandling av uppgifter till följd av särskilda omständigheter enligt den översändande medlemsstatens nationella lagstiftning är tillämpliga på utbyte av uppgifter mellan behöriga myndigheter inom den medlemsstaten, ska den översändande myndigheten informera mottagaren om dessa restriktioner. Även mottagaren ska se till att dessa restriktioner för behandling av uppgifter följs.
2. Vid tillämpning av punkt 1 ska medlemsstaterna inte tillämpa några andra restriktioner när det gäller överföringen av uppgifter till andra medlemsstater eller till myndigheter som inrättats i enlighet med avdelning VI i fördraget om Europeiska unionen än de som gäller motsvarande nationella överföringar av uppgifter.

Artikel 14

Överföring till behöriga myndigheter i tredjestater eller till internationella organ

1. Medlemsstaterna ska föreskriva att personuppgifter som översänts eller gjorts tillgängliga av den behöriga myndigheten i en annan medlemsstat får överföras till tredjestater eller internationella organ eller organisationer som inrättats genom internationella överenskommelser eller som förklarats vara internationella organ endast om
 - a) detta är nödvändigt för förebyggande, utredning, avslöjande eller lagföring av brott eller verkställighet av straffrättsliga påföljder,
 - b) den mottagande myndigheten i tredjestaten eller det mottagande internationella organet eller organisationen har ansvar för förebyggandet, utredningen, avslöjandet eller lagföringen av brott eller för verkställigheten av straffrättsliga påföljder,
 - c) den medlemsstat från vilken uppgifterna erhöles har gett sitt samtycke till överföringen i enlighet med sin nationella lagstiftning, och om
 - d) berörd tredjestat eller internationellt organ sörjer för en adekvat skyddsnivå för den avsedda databehandlingen.

2. Överföring utan förhandsmedgivande enligt punkt 1 c ska tillåtas endast om överföringen av uppgifter är absolut nödvändig för att kunna avvärja en direkt och allvarlig fara för den allmänna säkerheten i en medlemsstat eller en tredjestat eller för en medlemsstat väsentliga intressen och ett förhandsmedgivande inte kan erhållas i tid. Den myndighet som ansvarar för att bevilja medgivandet ska informeras utan dröjsmål.

3. Med avvikelse från punkt 1 d får personuppgifter överföras om
 - a) den nationella lagstiftningen i den medlemsstat som överför uppgifterna stadgar härom på grund av
 - i) de registrerade personernas legitima specifika intressen, eller
 - ii) legitima faktiska intressen, främst viktiga offentliga intressen, eller
 - b) tredjestaten eller mottagande internationella organ eller organisation sörjer för skyddsåtgärder som av den berörda medlemsstaten bedöms som tillräckliga i enlighet med dennas nationella lagstiftning.

4. Bedömningen av om den skyddsnivå som avses i punkt 1 d är adekvat ska ske på grundval av alla de förhållanden som har samband med en eller flera överföringar av personuppgifter. Särskild hänsyn ska tas till uppgifternas art, den föreslagna behandlingens eller behandlingarnas ändamål och varaktighet, ursprungsstaten och den stat eller internationella organisation som utgör slutdestination för uppgifterna, den lagstiftning, både allmän och sektoriell, som gäller i den berörda tredjestaten eller för den berörda internationella organisationen samt de yrkesregler och säkerhetsbestämmelser som där ska följas.

Artikel 14a

Överföring till privata parter i medlemsstaterna

1. Medlemsstaterna ska stadga om att personuppgifter som överförts från eller gjorts tillgängliga av den behöriga myndigheten i en annan medlemsstat endast får översändas till privata parter om
 - a) den behöriga myndigheten i den medlemsstat från vilken uppgifterna erhållits i enlighet med den nationella lagstiftning som gäller för denna har samtyckt till överföring,
 - b) inga legitima specifika intressen för den registrerade personen hindrar överföringen, och om
 - c) överföringen i särskilda fall är absolut nödvändig för den behöriga myndighet som översänder uppgifterna till en privat part för att denna ska kunna
 - i) utföra en uppgift den lagenligen tilldelats,
 - ii) förebygga, utreda, avslöja eller lagföra brott eller kunna verkställa straffrättsliga påföljder,
 - iii) avvärja en direkt och allvarlig fara för den allmänna säkerheten, eller
 - iv) förhindra att enskilda personers rättigheter lider allvarlig skada.
2. Den behöriga myndighet som översänder uppgifterna till en privat part ska meddela denna för vilka ändamål uppgifterna uteslutande får användas.

Artikel 15

Information på begäran av den behöriga myndigheten

Mottagaren ska på begäran informera den behöriga myndighet som har översänt uppgifter eller gjort dem tillgängliga om hur dessa behandlas.

Artikel 16
*Information till den registrerade personen*¹¹

1. Medlemsstaterna ska se till att den registrerade personen informeras om insamling eller behandling av personuppgifter av deras behöriga myndighet i enlighet med nationell lagstiftning.
2. Om personuppgifter har överförts eller gjorts tillgängliga mellan medlemsstaterna, får varje medlemsstat i enlighet med bestämmelserna i sin nationella lagstiftning enligt punkt 1, begära att den andra medlemsstaten inte informerar den registrerade personen. I sådana fall ska den senare medlemsstaten inte informera den registrerade personen utan förhandsmedgivande från den andra medlemsstaten.

Artikel 17
Rätt till tillgång

1. Varje registrerad person har rätt att på begäran, med rimliga intervall, utan hinder och utan större tidsutdräkt eller kostnader erhålla
 - a) åtminstone en bekräftelse från den registeransvarige eller från den behöriga nationella tillsynsmyndigheten av huruvida uppgifter som rör honom eller henne har överförts eller gjorts tillgängliga samt information om till vilka mottagare eller mottagarkategorier uppgifterna har lämnats ut och information om vilka uppgifter som behandlas, eller
 - b) åtminstone en bekräftelse från den behöriga nationella tillsynsmyndigheten av att alla nödvändiga kontroller har utförts.
2. Medlemsstaterna får anta lagstiftning som begränsar åtkomst till information enligt punkt 1 a, om denna begränsning med vederbörligt beaktande av vederbörandes legitima intressen är en nödvändig och rimlig åtgärd för att

¹¹ BG: Granskningsreservation. Reservation från CZ och SK.

- a) undgå att hindra officiella eller rättsliga utredningar, förundersökningar eller förfaranden,
 - b) undgå att skada förebyggande, upptäckt, utredning och lagföring av brott eller verkställighet av straffrättsliga påföljder,
 - c) skydda allmän säkerhet,
 - d) skydda nationell säkerhet,
 - e) skydda den registrerade eller andra personers fri- och rättigheter.
3. Varje vägran till tillgång eller begränsning av denna ska skriftligen meddelas den registrerade. De sakliga och rättsliga skäl som beslutet grundar sig på ska därvid också meddelas. Kravet på detta meddelande kan frångås om skäl enligt punkt 2 a–e föreligger. I samtliga dessa fall ska den registrerade meddelas att han eller hon kan överklaga till den behöriga nationella tillsynsmyndigheten, en rättslig myndighet eller domstol.

Artikel 18

Rätt till rättelse, radering eller blockering av uppgifter

1. Den registrerade har rätt att förvänta sig att den registeransvarige fullgör sin skyldighet enligt artiklarna 4, 9 och 10 att rätta, radera eller blockera personuppgifter som registrerats inom ramen för detta rambeslut. Medlemsstaterna ska fastställa huruvida den registrerade personen kan göra anspråk på denna rättighet direkt gentemot den registeransvarige eller via den behöriga nationella tillsynsmyndigheten. Om den registeransvarige vägrar att rätta, radera eller blockera måste vägran meddelas skriftligen och den registrerade personen måste informeras om de möjligheter som tillhandahålls inom den nationella lagstiftningen att anföra klagomål eller begära prövning. När klagomålet eller begäran om prövning behandlats ska den registrerade personen informeras om huruvida den registeransvarige handlat korrekt eller ej. Medlemsstaterna får även stadga att den registrerade personen endast ska informeras av den behöriga nationella tillsynsmyndigheten om att en genomgång har utförts.

2. Om den registrerade bestrider korrektheten av en personuppgift och det inte kan fastställas att denna är korrekt får denna uppgift markeras.

Artikel 19

Rätt till ersättning för skada

1. Var och en som lidit skada till följd av en otillåten behandling av personuppgifter eller av någon annan åtgärd som är oförenlig med de nationella bestämmelser som antagits till följd av detta rambeslut har rätt till ersättning av den registeransvarige eller av en annan myndighet som enligt nationell lagstiftning är ansvarig i fråga om den skada som han eller hon har lidit.
2. Om den behöriga myndigheten i en medlemsstat översänder personuppgifter kan mottagaren inte åberopa det faktum att de översända uppgifterna varit felaktiga för att undgå det ansvar som denne i enlighet med den nationella lagstiftningen har gentemot den skadelidande. Om mottagaren utbetalar skadestånd för en skada som vållats av att felaktigt översända uppgifter kommit till användning ska den översändande behöriga myndigheten ersätta mottagaren det skadestånd som utbetalats men därvid ta med i beräkningen eventuella felaktigheter som kan ha begåtts av mottagaren.

Artikel 20

Rättsmedel

Utan att det påverkar något administrativt förfarande som kan användas innan ett ärende anhängiggörs vid en rättslig instans ska den registrerade ha rätt att inför domstol föra talan mot kränkningar av sådana rättigheter som skyddas av den tillämpliga nationella lagstiftningen.

Artikel 21

Sekretess i samband med behandlingen av uppgifter

1. Var och en som får tillgång till personuppgifter som faller under tillämpningsområdet för detta rambeslut får endast behandla dessa i sin egenskap av anställda vid den behöriga myndigheten eller efter instruktioner från denna, såvida det inte föreligger rättsliga skyldigheter till annan behandling.
2. Var och en som anlitas för att arbeta för en behörig myndighet i en medlemsstat ska vara bunden av samtliga bestämmelser om skydd av uppgifter som gäller för respektive behörig myndighet.

Artikel 22

Säkerhet i samband med behandlingen av uppgifter

1. Medlemsstaterna ska se till att de behöriga myndigheterna vidtar lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifter från att utplånas genom olyckshändelse eller otillåtna handlingar och från att gå förlorade genom olyckshändelse samt från ändringar, otillåten spridning av eller otillåten tillgång till uppgifterna, särskilt om behandlingen innefattar överföring av uppgifter i ett nät och eller om uppgifterna gjorts tillgängliga genom direkt automatisk åtkomst, samt mot varje annat slag av otillåten behandling, varvid hänsyn särskilt ska tas till de risker som behandlingen innebär och arten av de uppgifter som ska skyddas. Dessa åtgärder ska med beaktande av den befintliga tekniska nivån och de kostnader som är förenade med åtgärdernas genomförande leda till att en lämplig säkerhetsnivå uppnås i förhållande till de risker som är förknippade med behandlingen och arten av de uppgifter som ska skyddas.
2. När det gäller automatisk databehandling ska varje medlemsstat vidta lämpliga åtgärder för att
 - a) förhindra att obehöriga kommer åt datorutrustning som används för behandling av personuppgifter (åtkomstskydd för utrustning),
 - b) förhindra att databärare läses, kopieras, ändras eller avlägsnas av obehöriga (databärarkontroll),

- c) förhindra obehörig lagring av uppgifter och obehörig åtkomst, ändring eller radering av lagrade personuppgifter (lagringskontroll),
 - d) förhindra att obehöriga kan använda system för automatisk databehandling med hjälp av utrustning för dataöverföring (användarkontroll),
 - e) se till att personer som är behöriga att använda ett system för automatisk databehandling endast har tillgång till uppgifter som omfattas av deras behörighet (åtkomstkontroll),
 - f) se till att det kan kontrolleras och fastställas till vilka organ personuppgifter har överförts eller kan överföras och för vilka organ uppgifterna har gjorts tillgängliga eller kan göras tillgängliga med hjälp av utrustning för dataöverföring (kommunikationskontroll),
 - g) se till att det finns möjlighet att i efterhand kontrollera och fastställa vilka personuppgifter som förts in i ett automatiskt databehandlingssystem, samt vid vilken tidpunkt och av vem uppgifterna infördes (indatakontroll),
 - h) förhindra obehörig läsning, kopiering, ändring eller radering av personuppgifter i samband med överföring av sådana uppgifter eller under transport av databärare (transportkontroll),
 - i) se till att de system som används kan repareras vid störningar (återställande),
 - j) se till att systemet fungerar, att funktionsfel rapporteras (driftsäkerhet) och att de lagrade uppgifterna inte kan förvrängas genom funktionsfel i systemet (dataintegritet).
3. Medlemsstaternas ska sörja för att endast sådana personer får utses till registerförare om vilka det kan garanteras att han eller hon vidtar de nödvändiga tekniska och organisatoriska åtgärderna enligt punkt 1 och beaktar anvisningarna i artikel 21. Den behöriga myndigheten ska övervaka registerföraren i detta avseende.

4. Personuppgifter får endast behandlas av en registerförare på grundval av en rättsakt eller ett skriftligt avtal.

Artikel 23

Föregående samråd

Medlemsstaterna ska sörja för att de behöriga nationella tillsynsmyndigheterna rådfrågas före behandling av personuppgifter i det nya register som ska inrättas om

- a) särskilda uppgiftskategorier enligt artikel 7 behandlas, eller om
- b) behandlingens typ, särskilt användning av ny teknik, nya mekanismer eller förfaranden, i övrigt innebär särskilda risker för registrerades grundläggande fri- och rättigheter och framför allt deras rätt till privatliv.

Artikel 24

Påföljder

Medlemsstaterna ska anta lämpliga bestämmelser för att säkerställa att detta rambeslut genomförs fullt ut och framför allt föreskriva effektiva, proportionella och avskräckande påföljder för överträdelse av bestämmelser som antagits i enlighet med detta rambeslut.

Artikel 25

Nationella tillsynsmyndigheter

1. Varje medlemsstat ska se till att det utses en eller flera myndigheter med uppgift att inom dess territorium vägleda och övervaka tillämpningen av de bestämmelser som medlemsstaterna antagit i enlighet med detta rambeslut. Dessa myndigheter ska vara fullt oberoende när de fullgör sina åligganden.

2. Varje tillsynsmyndighet ska bland annat ha
 - a) utredande befogenheter, som befogenhet att få tillgång till uppgifter som blir föremål för behandling och befogenhet att samla in all information som är nödvändig för att utföra tillsynen,
 - b) faktisk befogenhet att ingripa, som att kunna avge yttranden innan en behandling äger rum, att se till att sådana yttranden i lämplig omfattning offentliggörs, att kunna besluta om blockering, radering eller förstöring av uppgifter, att kunna besluta om tillfälligt eller slutligt förbud mot behandling, att kunna ge den registeransvarige en varning eller tillrättavisning eller att kunna hänskjuta frågor till nationella parlament eller andra politiska institutioner,
 - c) befogenhet att inleda rättsliga förfaranden när de nationella bestämmelser som antagits till följd av detta rambeslut har överträtts eller att uppmärksamma de rättsliga myndigheterna på dessa överträdelser. Beslut av tillsynsmyndigheten, som ger upphov till klagomål kan överklagas till domstol.
3. Var och en kan vända sig till tillsynsmyndigheten med en begäran om skydd för sina fri- och rättigheter med avseende på behandling av personuppgifter. Den berörda personen ska informeras om vilka följder hans begäran har fått.
4. Medlemsstaterna ska föreskriva att tillsynsmyndighetens ledamöter och personal även ska vara bundna av de för respektive behörig myndighet gällande bestämmelserna om skydd av uppgifter och ha tystnadsplikt med avseende på konfidentiell information som de har tillgång till även sedan deras uppdrag eller anställning upphört.

Artikel 27

Förhållande till avtal med tredjestater

Detta rambeslut ska inte påverka medlemsstaternas eller Europeiska unionens skyldigheter och åtaganden enligt de bilaterala och/eller multilaterala avtal med tredjestater som förelåg när rambeslutet antogs.

När dessa avtal tillämpas ska överföringen till en tredjestat av personuppgifter som erhållits från en annan medlemsstat genomföras med respekt för bestämmelserna i artikel 14.1 c och 14.2 om förhandsmedgivande.

Artikel 27a

Utvärdering

1. Tre år efter det att den period som fastställs i artikel 28.1 har löpt ut ska medlemsstaterna rapportera till kommissionen om de nationella åtgärder som de har vidtagit för att säkerställa fullständig efterlevnad av detta rambeslut, därvid även när det gäller de bestämmelser som redan ska följas när uppgifter samlas in. Kommissionen ska särskilt undersöka konsekvenserna av bestämmelsen om tillämpningsområdet i artikel 1.2.
2. Kommissionen ska inom ett år lämna rapport till rådet och Europaparlamentet om resultatet av den utvärdering som avses i punkt 1 och tillsammans med rapporten lämna lämpliga förslag till ändringar.

Artikel 27b

Förhållande till tidigare antagna unionsakter¹²

Om rättsakter som antagits enligt avdelning VI i fördraget om Europeiska unionen före det datum som avses i artikel 29 och som reglerar utbytet av personuppgifter mellan medlemsstaterna eller tillgång för medlemsstaternas utsedda myndigheter till informationssystem som inrättats enligt EG-fördraget innehåller särskilda villkor för den mottagande medlemsstatens användning av sådana uppgifter, ska dessa villkor ha företräde i förhållande till bestämmelserna i rambeslutet när det gäller användning av uppgifter som tagits emot eller gjorts tillgängliga av en annan medlemsstat.

Artikel 28

Genomförande

1. Medlemsstaterna ska vidta de åtgärder som är nödvändiga för att följa detta rambeslut senast två år efter det att detta har antagits.
2. Senast vid denna tidpunkt ska medlemsstaterna till rådets generalsekretariat och kommissionen överlämna texten till de bestämmelser genom vilka skyldigheterna enligt detta rambeslut införlivas med deras nationella lagstiftning samt upplysningar om den eller de tillsynsmyndigheter som avses i artikel 25. På grundval av denna information och en skriftlig rapport från kommissionen ska rådet före ... bedöma i vilken utsträckning medlemsstaterna har vidtagit de åtgärder som är nödvändiga för att följa detta rambeslut.

¹² Granskningsreservation från CZ och HU.

Artikel 29
Ikraftträdande

Detta rambeslut träder i kraft den tjugonde dagen efter det att det har offentliggjorts i Europeiska unionens officiella tidning.

Utfärdat i Bryssel den

På rådets vägnar
Ordförande

Utkast till rådsbeslut

UTKAST TILL UTTALANDE FRÅN RÅDET

"Rådet kommer att undersöka hur i framtiden de uppgifter som fullgörs av de befintliga gemensamma dataskyddsmyndigheter som var för sig inrättats för Schengens informationssystem, Europol, Eurojust och tullinformationssystemet, i enlighet med tillämpliga rättsliga grunder skulle kunna kombineras inom en enda dataskyddsmyndighet, vilket inbegriper den rådgivande funktionen, samtidigt som man beaktar dessa systems och organs specifika särart.

Rådet anser att detta är ett sätt att ytterligare förbättra organisationen av dataskyddet på området polissamarbete och straffrättsligt samarbete."
