



Ds 2005:50

Personuppgiftsbehandling hos Försvarsmakten och Försvarets radioanstalt



REGERINGSKANSLIET
Försvarsdepartementet





SOU och Ds kan köpas från Fritzes kundtjänst. För remissutsändningar av SOU och Ds svarar Fritzes Offentliga Publikationer på uppdrag av Regeringskansliets förvaltningsavdelning.

Beställningsadress:
Fritzes kundtjänst
106 47 Stockholm
Orderfax: 08-690 91 91
Ordertel: 08-690 91 90
E-post: order.fritzes@nj.se
Internet: www.fritzes.se

Svara på remiss. Hur och varför. Statsrådsberedningen, 2003.

– En liten broschyr som underlättar arbetet för den som skall svara på remiss.

Broschyren är gratis och kan laddas ner eller beställas på
<http://www.regeringen.se/remiss>

Tryckt av XGS Grafisk Service
Stockholm 2005

ISBN 91-38-22472-0
ISSN 0284-6012



Innehåll

Sammanfattning	9
1 Promemorians lagförslag	11
1.1 Förslag till lag om behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst.....	11
1.2 Förslag till lag om behandling av personuppgifter i Försvarets radioanstalts underrättelseverksamhet.....	25
2 Ärendet och dess beredning	37
3 Behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst	41
3.1 Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst.....	41
3.2 Den militära underrättelse- och säkerhetstjänstens organisation.....	47
3.3 Försvarmaktens informationshantering i den militära underrättelse- och säkerhetstjänsten	49
3.3.1 Behandling av personuppgifter	49

3.3.2	System för automatiserad behandling av personuppgifter.....	51
4	Behandling av personuppgifter i Försvarets radioanstalts underrättelseverksamhet m.m.....	55
4.1	Försvarets radioanstalts underrättelseverksamhet m.m.	55
4.2	Försvarets radioanstalts organisation	58
4.3	Försvarets radioanstalts informationshantering i underrättelseverksamheten m.m.	59
4.3.1	Behandling av personuppgifter i Försvarets radioanstalts underrättelseverksamhet m.m.....	59
4.3.2	System för automatiserad behandling av personuppgifter.....	60
5	Gällande rätt.....	65
5.1	Övergripande rättslig reglering av behandling av personuppgifter	65
5.1.1	Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna	65
5.1.2	Dataskyddskonventionen.....	66
5.1.3	Personuppgiftslagen	67
5.2	Rättslig reglering av behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst samt Försvarets radioanstalts underrättelseverksamhet.....	71
5.2.1	Gemensamma bestämmelser	71
5.2.2	Särskilda bestämmelser för Försvarsmaktens behandling av personuppgifter.....	72
5.2.3	Särskilda bestämmelser för Försvarets radioanstalts behandling av personuppgifter.....	73

6	Sammanfattning av förslagen i Ds 2005:30 En anpassad försvarsunderrättelseverksamhet.....	75
6.1	Förslag som rör försvarsunderrättelseverksamheten.....	75
6.2	Förslag till lag om signalspaning.....	77
7	Allmänna utgångspunkter	81
7.1	Särskild författningsreglering.....	81
7.2	Lagarnas förhållande till personuppgiftslagen.....	84
7.3	Lagarnas allmänna tillämpningsområde.....	90
7.4	Syftet med lagarna.....	93
7.5	Författningsstruktur.....	94
8	Bestämmelser om behandling av personuppgifter	95
8.1	Förhållandet till offentlighetsprincipen.....	95
8.2	Definitioner.....	96
8.3	Personuppgiftsansvar.....	99
8.4	Grundläggande krav på behandling av personuppgifter.....	100
8.5	När behandling av personuppgifter är tillåten	107
8.6	Personuppgifter som får behandlas inom den militära säkerhetstjänsten.....	118
8.6.1	Grunder för behandling i den militära säkerhetstjänsten av uppgifter om en person.....	118
8.6.2	Signalkontrollverksamhet	121
8.7	Behandling av känsliga personuppgifter	123
8.8	Behandling av personnummer.....	127

8.9	Behandling av personuppgifter i vissa fall.....	128
8.10	Överföring av personuppgifter till andra länder	130
8.11	Information till den enskilde.....	135
8.12	Rättelse	141
8.13	Skadestånd	143
8.14	Säkerheten vid behandling.....	144
8.15	Personuppgiftsombud m.m.	147
8.16	Tillsyn och särskild granskning till skydd för den personliga integriteten	151
8.17	Tillsynsmyndighetens och det särskilda granskningsorganets befogenheter	158
8.18	Straff 160	
8.19	Överklagande.....	163
8.20	Bevarande och gallring	166
8.21	Utlämnande av uppgifter	174
8.21.1	Sekretess och utlämnande av uppgifter till utländsk myndighet eller internationell organisation.....	174
8.21.2	Utlämnande av personuppgifter på medium för automatiserad behandling.....	176
8.21.3	Direktåtkomst.....	178
8.22	Bestämmelser i personuppgiftslagen som inte upprepas.....	181
9	Särskilda bestämmelser för samlingar av uppgifter....	185
9.1	Samlingar av uppgifter	185
9.2	Uppgifter som får behandlas	189

10	Ikraftträdande och övergångsbestämmelser	191
11	Konsekvensbeskrivning	193
12	Författningskommentar	195
12.1	Förslag till lag om behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst	195
12.2	Förslag till lag om behandling av personuppgifter i Försvarets radioanstalts underrättelseverksamhet	215
Bilaga 1	223
Bilaga 2	237
Bilaga 3	251

Sammanfattning

Promemorian innehåller förslag till dels en ny lag om behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst, dels en ny lag om behandling av personuppgifter i Försvarets radioanstalts underrättelseverksamhet. Lagförslagen är heltäckande och innehåller således alla de bestämmelser som skall vara tillämpliga för Försvarmaktens och Försvarets radioanstalts behandling av personuppgifter inom ramen för de aktuella verksamheterna. Lagförslagen föreslås träda ikraft den 1 januari 2007.

1 Promemorians lagförslag

1.1 Förslag till lag om behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst

1 kap. Allmänna bestämmelser

Lagens tillämpningsområde m.m.

1 § Denna lag gäller vid behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst, om behandlingen är helt eller delvis automatiserad eller om uppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

Personuppgiftslagen (1998:204) gäller inte vid sådan behandling av personuppgifter som anges i första stycket.

2 § Syftet med lagen är att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst.

Förhållandet till offentlighetsprincipen

3 § Bestämmelserna i denna lag tillämpas inte i den utsträckning det skulle inskränka Försvarsmaktens skyldighet enligt 2 kap. tryckfrihetsförordningen att lämna ut personuppgifter.

Definitioner

4 § I denna lag används följande beteckningar med nedan angiven betydelse.

<i>Beteckning</i>	<i>Betydelse</i>
<i>Behandling</i> (<i>av personuppgifter</i>)	Varje åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter, vare sig det sker på automatisk väg eller inte, t.ex. insamling, registrering, organisering, lagring, bearbetning eller ändring, återvinning, inhämtande, användning, utlämnande genom översändande, spridning eller annat tillhandahållande av uppgifter, sammanställning eller samkörning, blockering, utplåning eller förstöring.
<i>Blockering</i> (<i>av personuppgifter</i>)	En åtgärd som vidtas för att personuppgifterna skall vara förknippade med information om att de är spärrade och om anledningen till spärren och för att personuppgifterna inte skall lämnas ut till tredje man annat än med stöd av 2 kap. tryckfrihetsförordningen.
<i>Mottagare</i>	Den till vilken personuppgifter lämnas ut. När personuppgifter lämnas ut från Försvarsmakten för att en annan myn-

dighet skall kunna utföra sådan tillsyn, kontroll eller revision som den är skyldig att sköta, anses dock inte den myndigheten som mottagare.

Personuppgifter All slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet.

Personuppgiftsbiträde Den som behandlar personuppgifter för den personuppgiftsansvariges räkning.

Personuppgiftsombud Den fysiska person som, efter förordnande av den personuppgiftsansvarige, självständigt skall se till att personuppgifter behandlas på ett korrekt och lagligt sätt.

Den registrerade Den som en personuppgift avser.

Tredje man Någon annan än den registrerade, den personuppgiftsansvarige, personuppgiftsombudet, personuppgiftsbiträdet och sådana personer som under den personuppgiftsansvariges eller personuppgiftsbitrådets direkta ansvar har befogenhet att behandla personuppgifter.

Personuppgiftsansvar

5 § Försvarsmakten är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför. Försvarsmakten bestämmer medlen för och, inom ramen för 7 och 8 §§, ändamålen med behandlingen av personuppgifter.

Grundläggande krav på behandling av personuppgifter

6 § Försvarsmakten skall se till att

1. personuppgifter alltid behandlas på ett korrekt sätt och i enlighet med god sed,
2. personuppgifter samlas in bara för särskilda, uttryckligt angivna och berättigade ändamål,
3. personuppgifter inte behandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in,
4. de personuppgifter som behandlas är adekvata och relevanta i förhållande till ändamålen med behandlingen,
5. inte fler personuppgifter behandlas än som är nödvändigt med hänsyn till ändamålen med behandlingen,
6. de personuppgifter som behandlas är riktiga och, om det är nödvändigt, aktuella, och
7. alla rimliga åtgärder vidtas för att rätta, blockera eller utplåna sådana personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålen med behandlingen.

När behandling av personuppgifter är tillåten

Försvarsunderrättelseverksamhet

7 § Personuppgifter får behandlas i Försvarsmaktens försvarsunderrättelseverksamhet om det är nödvändigt för att bedriva den verksamhet som anges i lagen (2000:130) om försvarsunderrättelseverksamhet.

Uppgifter om en person får endast behandlas om personen har anknytning till en preciserad inriktning för försvarsunderrättelseverksamheten och behandlingen är nödvändig för att fullfölja den inriktningen.

Den militära säkerhetstjänsten

8 § Personuppgifter får behandlas i Försvarsmaktens militära säkerhetstjänst för att upptäcka, förebygga och avvärja säker-

hetsshotande verksamhet som riktas mot Försvarmakten och dess säkerhetsintressen, om det är nödvändigt för att

1. klarlägga verksamhet som innefattar hot mot rikets säkerhet, eller
2. vidta åtgärder som hindrar eller försvårar säkerhetsshotande verksamhet.

9 § Uppgifter om en person får behandlas för de ändamål som anges i 8 § endast enligt 10 § eller om

1. uppgifterna ger grundad anledning anta att personen utövat eller kan komma att utöva verksamhet som innefattar sådant hot mot rikets säkerhet som utgör brott eller terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott eller motsvarande brottslighet enligt tidigare lagstiftning,

2. uppgifterna ger grundad anledning anta att personen utövat eller kan komma att utöva underrättelseverksamhet riktad mot Försvarmakten och dess säkerhetsintressen,

3. uppgifterna ger grundad anledning anta att personen utövar annan säkerhetsshotande verksamhet än som avses i 1 och som innefattar brott eller åsidosättande av åligganden i anställning hos Försvarmakten, och det finns särskilda skäl till att uppgiften skall behandlas,

4. personen har lämnat uppgifter om säkerhetsshotande verksamhet och personuppgifterna är nödvändiga för att bedöma personens trovärdighet, eller

5. uppgifterna avser information som har framkommit i samband med att en person har genomgått registerkontroll eller särskild personutredning enligt säkerhetsskyddslagen (1996:627).

Uppgifter om en person skall förse med upplysning om på vilken av de i första stycket angivna grunderna uppgiften behandlas. Om behandlingen av en personuppgift föranleds av annat än antagande om att personen har utövat eller kommer att utöva brottslig verksamhet skall det särskilt anges att personen inte är misstänkt för brottslig verksamhet, om det inte på annat sätt klart framgår att sådan misstanke inte finns. Uppgifter om en person som inte heller kan antas ha utövat eller komma att

utöva annan säkerhetshotande verksamhet skall förses med en särskild upplysning om detta, om det inte på annat sätt klart framgår att sådant antagande inte finns.

Uppgifter om en person som avses i punkterna 1–3 skall förses med en upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak.

10 § Personuppgifter som ingår i eller har uppkommit i samband med användning av totalförsvarets telekommunikations- och informationssystem får behandlas för att förhindra obehörig insyn i och påverka av dessa system. Det gäller även sådana uppgifter som avses i 11 och 12 §§. Behandling som särskilt syftar till att identifiera en person får dock endast utföras om det finns grundad anledning att anta att det beträffande personen föreligger sådant förhållande som avses i 9 § första stycket 1, 2 eller 3.

Försvarsmakten skall föra en förteckning över de behandlingar som särskilt syftar till att identifiera en person och de uppgifter som utgjort anledningen till behandlingen.

Behandling av känsliga personuppgifter

11 § Personuppgifter får inte behandlas enbart på grund av vad som är känt om personens ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexualliv.

Om uppgifter om en person behandlas på annan grund får de kompletteras med sådana uppgifter som avses i första stycket när det är oundgängligen nödvändigt för syftet med behandlingen. Uppgifter som beskriver en persons utseende skall alltid utformas på ett objektivet sätt med respekt för människovärdet.

Vid sökning får personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening eller som rör hälsa eller sexualliv användas som sökbegrepp endast om det är oundgängligen nödvändigt för syftet med behandlingen.

Behandling av personnummer

12 § Uppgifter om personnummer eller samordningsnummer får behandlas bara när det är klart motiverat med hänsyn till

- a) ändamålet med behandlingen,
- b) vikten av en säker identifiering, eller
- c) något annat beaktansvärt skäl.

Utlämnande av personuppgifter på medium för automatiserad behandling

13 § Enstaka personuppgifter får lämnas ut på medium för automatiserad behandling. Annars får utlämnande på sådant medium ske endast om regeringen har meddelat föreskrifter eller beslut om det.

Direktåtkomst

14 § Vilka som får ha direktåtkomst till personuppgifter bestäms av regeringen i förordning eller beslut.

Regeringen, eller den myndighet regeringen bestämmer, meddelar närmare föreskrifter eller beslut om omfattningen av direktåtkomsten.

Tillgången till personuppgifter

15 § Tillgången till personuppgifter skall alltid begränsas till vad personen behöver för att kunna fullgöra sina arbetsuppgifter.

Överföring av personuppgifter till andra länder

16 § Personuppgifter som behandlas med stöd av denna lag får föras över till andra länder endast om sekretess inte hindrar det

och det är nödvändigt för att Försvarsmakten skall kunna fullgöra sina uppgifter inom ramen för det internationella försvarsunderrättelse- och säkerhetssamarbetet.

Regeringen får föreskriva eller i särskilt fall besluta att överföring även får ske i andra fall om det är nödvändigt för att Försvarsmakten skall kunna fullgöra sina uppgifter.

Uppgiftssamlingar

17 § I Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst får det under de förutsättningar som anges i 6-16 § finnas ett antal skilda samlingar uppgifter som med hjälp av automatiserad behandling används gemensamt i respektive verksamhet för de i 7 och 8 §§ angivna ändamålen.

Regeringen meddelar närmare föreskrifter eller beslut om vilka uppgiftssamlingar enligt första stycket som får finnas och vilka uppgifter som får behandlas i respektive samling.

2 kap. Information till den enskilde, rättelse och skadestånd

Information till den enskilde

Information skall lämnas självmant

1 § Om uppgifter om en person samlas in i den militära säkerhetstjänsten från personen själv skall Försvarsmakten i samband därmed självmant lämna den registrerade information om behandlingen av uppgifterna. Informationen skall omfatta

1. uppgift om att det är Försvarsmakten som är personuppgiftsansvarig för behandlingen,
2. uppgift om ändamålen med behandlingen, och
3. all övrig information som behövs för att den registrerade skall kunna ta till vara sina rättigheter i samband med behandlingen, såsom information om mottagarna av uppgifterna, skyldighet att lämna uppgifter och rätten att ansöka om information och få rättelse.

Information enligt första stycket behöver inte lämnas om sådant som den registrerade redan känner till.

Information skall lämnas efter ansökan

2 § Försvarsmakten är skyldig att till var och en som ansöker om det en gång per kalenderår gratis lämna besked om personuppgifter som rör den sökande behandlas eller ej. Behandlas sådana uppgifter skall skriftlig information lämnas också om

1. vilka uppgifter om den sökande som behandlas,
2. varifrån dessa uppgifter har hämtats,
3. ändamålen med behandlingen, och
4. till vilka mottagare eller kategorier av mottagare som uppgifterna lämnas ut.

En ansökan enligt första stycket skall göras skriftligen hos Försvarsmakten och vara undertecknad av den sökande själv. Information enligt första stycket skall lämnas inom en månad från det att ansökan gjordes. Om det finns särskilda skäl för det, får information dock lämnas senast fyra månader efter det att ansökan gjordes.

3 § Information enligt 2 § behöver inte lämnas i den utsträckning detta visar sig vara omöjligt eller skulle innebära en oproportionerligt stor arbetsinsats.

Sådan information behöver inte heller lämnas om personuppgifter i löpande text som inte fått sin slutliga utformning när ansökan gjordes eller som utgör minnesanteckning eller liknande. Vad som nu sagts gäller dock inte om uppgifterna har lämnats ut till tredje man eller, när det gäller löpande text som inte fått sin slutliga utformning, om uppgifterna har behandlats under längre tid än ett år.

Undantag från informationsskyldigheten vid sekretess

4 § Bestämmelserna i 1 och 2 §§ gäller inte i den utsträckning sekretess hindrar att uppgifterna lämnas ut till den registrerade.

Rättelse

5 § Försvarsmakten är skyldig att på begäran av den registrerade snarast rätta, blockera eller utplåna sådana personuppgifter som inte har behandlats i enlighet med denna lag eller föreskrifter som har utfärdats med stöd av lagen. Försvarsmakten skall också underrätta tredje man till vilken uppgifterna har lämnats ut om åtgärden, om den registrerade begär det eller om mera betydande skada eller olägenhet för den registrerade skulle kunna undvikas genom en underrättelse. Någon sådan underrättelse behöver dock inte lämnas, om detta visar sig vara omöjligt eller skulle innebära en oproportionerligt stor arbetsinsats.

Skadestånd

6 § Staten skall ersätta den registrerade för skada och kränkning av den personliga integriteten som en behandling av personuppgifter i strid med denna lag har orsakat.

Ersättningskyldigheten kan i den utsträckning det är skäligt jämkas, om Försvarsmakten visar att felet inte berodde på myndigheten.

3 kap. Säkerheten vid behandling

1 § Ett personuppgiftsbiträde och den eller de personer som arbetar under bitrådets eller Försvarsmaktens ledning får behandla personuppgifter bara i enlighet med instruktioner från Försvarsmakten.

Det skall finnas ett skriftligt avtal om personuppgiftsbitrådets behandling av personuppgifter för Försvarsmaktens räkning. I

det avtalet skall det särskilt föreskrivas att personuppgiftsbiträdet får behandla personuppgifterna bara i enlighet med instruktioner från Försvarmakten och att personuppgiftsbiträdet är skyldigt att vidta de åtgärder som avses i 2 § första stycket.

I fråga om sekretess och tystnadsplikt i det allmännas verksamhet tillämpas bestämmelserna i sekretesslagen (1980:100) i stället för vad som sägs i första stycket.

2 § Försvarmakten skall vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna skall åstadkomma en säkerhetsnivå som är lämplig med beaktande av

1. de tekniska möjligheter som finns,
2. vad det skulle kosta att genomföra åtgärderna,
3. de särskilda risker som finns med behandlingen av personuppgifterna, och
4. hur pass känsliga de behandlade personuppgifterna är.

När Försvarmakten anlitar ett personuppgiftsbiträde, skall Försvarmakten förvissa sig om att personuppgiftsbiträdet kan genomföra de säkerhetsåtgärder som måste vidtas och se till att personuppgiftsbiträdet verkligen vidtar åtgärderna.

4 kap. Personuppgiftsombud

1 § Försvarmakten skall utse ett eller flera personuppgiftsombud och anmäla dessa till den tillsynsmyndighet som avses i 5 kap. Även ett entledigande av ett personuppgiftsombud skall anmälas till tillsynsmyndigheten.

2 § Personuppgiftsombudet skall ha till uppgift att självständigt se till att Försvarmakten behandlar personuppgifter på ett lagligt och korrekt sätt och i enlighet med god sed samt påpeka eventuella brister för myndigheten.

Har personuppgiftsombudet anledning att misstänka att Försvarmakten bryter mot de bestämmelser som gäller för behandlingen av personuppgifter och vidtas inte rättelse så snart det kan

ske efter påpekande, skall personuppgiftsombudet anmäla förhållandet till tillsynsmyndigheten.

Personuppgiftsombudet skall även i övrigt samråda med tillsynsmyndigheten vid tveksamhet om hur de bestämmelser som gäller för behandlingen av personuppgifter skall tillämpas.

3 § Personuppgiftsombudet skall över de behandlingar som Försvarsmakten genomför och som är helt eller delvis automatiserade föra en förteckning som avser försvarsunderrättelseverksamheten och en förteckning som avser den militära säkerhetstjänsten.

Regeringen eller den myndighet regeringen bestämmer meddelar närmare föreskrifter om vad förteckningen skall innehålla.

4 § Personuppgiftsombudet skall hjälpa registrerade att få rättelse när det finns anledning att misstänka att behandlade personuppgifter är felaktiga eller ofullständiga.

5 kap. Tillsynsmyndigheten

1 § Den myndighet som regeringen bestämmer skall utöva tillsyn över Försvarsmaktens behandling av personuppgifter enligt denna lag.

2 § Tillsynsmyndigheten har rätt att för sin tillsyn på begäran få

1. tillgång till de personuppgifter som behandlas,
2. upplysningar om och dokumentation av behandlingen av personuppgifter och säkerheten vid denna, och
3. tillträde till sådana lokaler som har anknytning till behandlingen av personuppgifter.

3 § Om tillsynsmyndigheten konstaterar att personuppgifter behandlas eller kan komma att behandlas på ett olagligt sätt, skall myndigheten genom påpekanden eller liknande förfaranden försöka åstadkomma rättelse.

4 § Tillsynsmyndigheten får hos länsrätten i Stockholms län ansöka om att sådana personuppgifter som har behandlats på ett olagligt sätt skall utplånas.

Beslut om utplånande får inte meddelas om det är oskäligt.

6 kap. Övriga bestämmelser

Gallring

1 § Personuppgifter som behandlas automatiserat skall gallras så snart uppgifterna inte längre behövs för det ändamål för vilket de behandlas. Regeringen får dock meddela föreskrifter eller beslut om att gallring skall ske senast vid viss tidpunkt.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om att personuppgifter utan hinder av första stycket får bevaras för historiska, statistiska och vetenskapliga ändamål.

Straff

2 § Till böter eller fängelse i högst sex månader eller, om brottet är grovt, till fängelse i högst två år döms den som uppsåtligen eller av grov oaktsamhet

a) lämnar osann uppgift i sådan information till registrerade som föreskrivs i denna lag, i anmälan till tillsynsmyndigheten enligt 4 kap. 1 § eller till tillsynsmyndigheten när myndigheten begär information enligt 5 kap. 1 § eller

b) behandlar personuppgifter i strid med 1 kap. 11 §.

I ringa fall döms inte till ansvar.

Överklagande

3 § Försvarsmaktens beslut om information som skall lämnas enligt 2 kap. 1 och 2 §§ och om rättelse enligt 2 kap. 5 § får över-

klagas hos allmän förvaltningsdomstol. Andra beslut enligt denna lag får inte överklagas.

Prövningstillstånd krävs vid överklagande till kammarrätten.

1. Denna lag träder i kraft den 1 januari 2007.

2. Bestämmelser i lagen om grundläggande krav på behandling av personuppgifter samt behandling av känsliga personuppgifter skall inte börja tillämpas förrän den 1 oktober 2007 i fråga om sådan manuell behandling av personuppgifter som påbörjats före den 24 oktober 1998 eller manuell behandling som utförs för ett visst bestämt ändamål om manuell behandling för ändamålet påbörjats före den 24 oktober 1998.

1.2 Förslag till lag om behandling av personuppgifter i Försvarets radioanstalts underrättelseverksamhet

1 kap. Allmänna bestämmelser

Lagens tillämpningsområde m.m.

1 § Denna lag gäller vid behandling av personuppgifter i Försvarets radioanstalts underrättelse- och utvecklingsverksamhet, om behandlingen är helt eller delvis automatiserad eller om uppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

Personuppgiftslagen (1998:204) gäller inte vid sådan behandling av personuppgifter som anges i första stycket.

2 § Syftet med lagen är att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter i Försvarets radioanstalts underrättelse- och utvecklingsverksamhet.

Förhållandet till offentlighetsprincipen

3 § Bestämmelserna i denna lag tillämpas inte i den utsträckning det skulle inskränka Försvarets radioanstalts skyldighet enligt 2 kap. tryckfrihetsförordningen att lämna ut personuppgifter.

Definitioner

4 § I denna lag används följande beteckningar med nedan angiven betydelse.

<i>Beteckning</i>	<i>Betydelse</i>
<i>Behandling</i> (av personuppgifter)	Varje åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter, vare sig det sker på automatisk väg eller inte, t.ex. insamling, registrering, organisering, lagring, bearbetning eller ändring, återvinning, inhämtande, användning, utlämnande genom översändande, spridning eller annat tillhandahållande av uppgifter, sammanställning eller samkörning, blockering, utplåning eller förstöring.
<i>Blockering</i> (av personuppgifter)	En åtgärd som vidtas för att personuppgifterna skall vara förknippade med information om att de är spärrade och om anledningen till spärren och för att personuppgifterna inte skall lämnas ut till tredje man annat än med stöd av 2 kap. tryckfrihetsförordningen.
<i>Mottagare</i>	Den till vilken personuppgifter lämnas ut. När personuppgifter lämnas ut från Försvarets radioanstalt för att en annan myndighet skall kunna utföra sådan tillsyn, kontroll eller revision som den är skyldig att sköta, anses dock inte den myndigheten som mottagare.
<i>Personuppgifter</i>	All slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet.
<i>Personuppgiftsbiträde</i>	Den som behandlar personuppgifter för

den personuppgiftsansvariges räkning.

Personuppgiftsombud Den fysiska person som, efter förordnande av den personuppgiftsansvarige, självständigt skall se till att personuppgifter behandlas på ett korrekt och lagligt sätt.

Den registrerade Den som en personuppgift avser.

Tredje man Någon annan än den registrerade, den personuppgiftsansvarige, personuppgiftsombudet, personuppgiftsbiträdet och sådana personer som under den personuppgiftsansvariges eller personuppgiftsbitrådets direkta ansvar har befogenhet att behandla personuppgifter.

Personuppgiftsansvar

5 § Försvarets radioanstalt är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför. Försvarets radioanstalt bestämmer medlen för och, inom ramen för 7–9 §§, ändamålen med behandlingen av personuppgifter.

Grundläggande krav på behandling av personuppgifter

6 § Försvarets radioanstalt skall se till att

1. personuppgifter alltid behandlas på ett korrekt sätt och i enlighet med god sed,
2. personuppgifter samlas in bara för särskilda, uttryckligt angivna och berättigade ändamål,

3. personuppgifter inte behandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in,
4. de personuppgifter som behandlas är adekvata och relevanta i förhållande till ändamålen med behandlingen,
5. inte fler personuppgifter behandlas än som är nödvändigt med hänsyn till ändamålen med behandlingen,
6. de personuppgifter som behandlas är riktiga och, om det är nödvändigt, aktuella, och
7. alla rimliga åtgärder vidtas för att rätta, blockera eller utplåna sådana personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålen med behandlingen.

När behandling av personuppgifter är tillåten

Underrättelseverksamhet

7 § Personuppgifter får behandlas i Försvarets radioanstalts försvarsunderrättelseverksamhet om det är nödvändigt för att bedriva den verksamhet som anges i lagen (2000:130) om försvarsunderrättelseverksamhet.

Uppgifter om en person får endast behandlas om personen har anknytning till en preciserad inriktning för försvarsunderrättelseverksamheten och behandlingen är nödvändig för att fullfölja den inriktningen.

8 § Personuppgifter får vidare behandlas av Försvarets radioanstalt i sådan underrättelseverksamhet som inte omfattas av 7 §, om det är nödvändigt för att, i enlighet med vad regeringen bestämmer,

1. följa förändringar av signalmiljön i omvärlden, den tekniska utvecklingen och signalskyddet, samt
2. fortlöpande utveckla den teknik och metodik som behövs för att bedriva verksamheten.

Utvecklingsverksamhet

9 § Personuppgifter får behandlas av Försvarets radioanstalt om det är nödvändigt för att biträda andra myndigheter vid värdering, utveckling, anskaffning och drift av signalspaningssystem. Personuppgifterna får inte användas för något annat ändamål eller lämnas ut till annan.

Behandling av känsliga personuppgifter

10 § Personuppgifter får inte behandlas enbart på grund av vad som är känt om personens ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexualliv.

Om uppgifter om en person behandlas på annan grund får de kompletteras med sådana uppgifter som avses i första stycket när det är oundgängligen nödvändigt för syftet med behandlingen. Uppgifter som beskriver en persons utseende skall alltid utformas på ett objektivt sätt med respekt för människovärdet.

Vid sökning får personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening eller som rör hälsa eller sexualliv användas som sökbegrepp endast om det är oundgängligen nödvändigt för syftet med behandlingen.

Behandling av personnummer

11 § Uppgifter om personnummer eller samordningsnummer får behandlas bara när det är klart motiverat med hänsyn till

- a) ändamålet med behandlingen,
- b) vikten av en säker identifiering, eller
- c) något annat beaktansvärt skäl.

Utlämnande av personuppgifter på medium för automatiserad behandling

12 § Enstaka personuppgifter får lämnas ut på medium för automatiserad behandling. Annars får utlämnande på sådant medium ske endast om regeringen har meddelat föreskrifter eller beslut om det.

Direktåtkomst

13 § Vilka som får ha direktåtkomst till personuppgifter bestäms av regeringen i förordning eller beslut.

Regeringen, eller den myndighet regeringen bestämmer, meddelar närmare föreskrifter eller beslut om omfattningen av direktåtkomsten.

Tillgången till personuppgifter

14 § Tillgången till personuppgifter skall alltid begränsas till vad personen behöver för att kunna fullgöra sina arbetsuppgifter.

Behandling av personuppgifter i vissa fall

15 § Behandling som innebär inhämtning av personuppgifter genom signalspaning, lagring av uppgifter som sker omedelbart därefter samt bearbetning av information i form av kryptoforcering och språklig översättning skall inte anses som oförenlig med bestämmelserna i 6–11 §§ i det skede av behandlingen under vilket det ännu inte kunnat fastställas om den inhämtade, lagrade eller bearbetade informationen innehåller personuppgifter.

Överföring av personuppgifter till andra länder

16 § Personuppgifter som behandlas med stöd av denna lag får föras över till andra länder om sekretess inte hindrar det och det är nödvändigt för att Försvarets radioanstalt skall kunna fullgöra sina uppgifter inom ramen för det internationella försvarsunder rättelse- och säkerhetssamarbetet.

Regeringen får föreskriva eller i särskilt fall besluta att överföring även får ske i andra fall om det är nödvändigt för att Försvarets radioanstalt skall kunna fullgöra sina uppgifter.

Uppgiftssamlingar

17 § I Försvarets radioanstalts underrättelseverksamhet får det under de förutsättningar som anges i 6-16 § finnas ett antal skilda samlingar uppgifter som med hjälp av automatiserad behandling används gemensamt i respektive verksamhet för de i 7-9 §§ angivna ändamålen.

Regeringen meddelar närmare föreskrifter eller beslut om vilka uppgiftssamlingar enligt första stycket som får finnas och vilka uppgifter som får behandlas i respektive samling.

2 kap. Information till den enskilde, rättelse och skadestånd

Information till den enskilde

Information skall lämnas efter ansökan

1 § Försvarets radioanstalt är skyldig att till var och en som ansöker om det en gång per kalenderår gratis lämna besked om personuppgifter som rör den sökande behandlas eller ej. Behandlas sådana uppgifter skall skriftlig information lämnas också om

1. vilka uppgifter om den sökande som behandlas,
2. varifrån dessa uppgifter har hämtats,
3. ändamålen med behandlingen, och

4. till vilka mottagare eller kategorier av mottagare som uppgifterna lämnas ut.

En ansökan enligt första stycket skall göras skriftligen hos Försvarets radioanstalt och vara undertecknad av den sökande själv. Information enligt första stycket skall lämnas inom en månad från det att ansökan gjordes. Om det finns särskilda skäl för det, får information dock lämnas senast fyra månader efter det att ansökan gjordes.

2 § Information enligt 1 § behöver inte lämnas i den utsträckning detta visar sig vara omöjligt eller skulle innebära en oproportionerligt stor arbetsinsats.

Sådan information behöver inte heller lämnas om personuppgifter i löpande text som inte fått sin slutliga utformning när ansökan gjordes eller som utgör minnesanteckning eller liknande. Vad som nu sagts gäller dock inte om uppgifterna har lämnats ut till tredje man eller, när det gäller löpande text som inte fått sin slutliga utformning, om uppgifterna har behandlats under längre tid än ett år.

Undantag från informationsskyldigheten vid sekretess

3 § Bestämmelserna i 1 § gäller inte i den utsträckning sekretess hindrar att uppgifterna lämnas ut till den registrerade.

Rättelse

4 § Försvarets radioanstalt är skyldig att på begäran av den registrerade snarast rätta, blockera eller utplåna sådana personuppgifter som inte har behandlats i enlighet med denna lag eller föreskrifter som har utfärdats med stöd av lagen. Försvarets radioanstalt skall också underrätta tredje man till vilken uppgifterna har lämnats ut om åtgärden, om den registrerade begär det eller om mera betydande skada eller olägenhet för den registrerade skulle kunna undvikas genom en underrättelse. Någon sådan un-

derrättelse behöver dock inte lämnas, om detta visar sig vara omöjligt eller skulle innebära en oproportionerligt stor arbetsinsats.

Skadestånd

5 § Staten skall ersätta den registrerade för skada och kränkning av den personliga integriteten som en behandling av personuppgifter i strid med denna lag eller föreskrifter som har utfärdats med stöd av lagen har orsakat.

Ersättningsskyldigheten kan i den utsträckning det är skäligt jämkas, om Försvarets radioanstalt visar att felet inte berodde på myndigheten.

3 kap. Säkerheten vid behandling

1 § Ett personuppgiftsbiträde och den eller de personer som arbetar under bitrådets eller Försvarets radioanstalts ledning får behandla personuppgifter bara i enlighet med instruktioner från Försvarets radioanstalt.

Det skall finnas ett skriftligt avtal om personuppgiftsbitrådets behandling av personuppgifter för Försvarets radioanstalts räkning. I det avtalet skall det särskilt föreskrivas att personuppgiftsbiträdet får behandla personuppgifterna bara i enlighet med instruktioner från Försvarets radioanstalt och att personuppgiftsbiträdet är skyldigt att vidta de åtgärder som avses i 2 § första stycket.

I fråga om sekretess och tystnadsplikt i det allmännas verksamhet tillämpas bestämmelserna i sekretesslagen (1980:100) i stället för vad som sägs i första stycket.

2 § Försvarets radioanstalt skall vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna skall åstadkomma en säkerhetsnivå som är lämplig med beaktande av

1. de tekniska möjligheter som finns,
2. vad det skulle kosta att genomföra åtgärderna,
3. de särskilda risker som finns med behandlingen av personuppgifterna, och
4. hur pass känsliga de behandlade personuppgifterna är.

När Försvarets radioanstalt anlitar ett personuppgiftsbiträde, skall myndigheten förvissa sig om att personuppgiftsbiträdet kan genomföra de säkerhetsåtgärder som måste vidtas och se till att personuppgiftsbiträdet verkligen vidtar åtgärderna.

4 kap. Personuppgiftsombud

1 § Försvarets radioanstalt skall utse ett eller flera personuppgiftsombud och anmäla dessa till den tillsynsmyndighet som avses i 5 kap. Även ett entledigande av ett personuppgiftsombud skall anmälas till tillsynsmyndigheten.

2 § Personuppgiftsombudet skall ha till uppgift att självständigt se till att Försvarets radioanstalt behandlar personuppgifter på ett lagligt och korrekt sätt och i enlighet med god sed samt påpeka eventuella brister för myndigheten.

Har personuppgiftsombudet anledning att misstänka att Försvarets radioanstalt bryter mot de bestämmelser som gäller för behandlingen av personuppgifter och vidtas inte rättelse så snart det kan ske efter påpekande, skall personuppgiftsombudet anmäla förhållandet till tillsynsmyndigheten.

Personuppgiftsombudet skall även i övrigt samråda med tillsynsmyndigheten vid tveksamhet om hur de bestämmelser som gäller för behandlingen av personuppgifter skall tillämpas.

3 § Personuppgiftsombudet skall föra en förteckning över de behandlingar som Försvarets radioanstalt genomför och som är helt eller delvis automatiserade.

Regeringen eller den myndighet regeringen bestämmer meddelar närmare föreskrifter om vad förteckningen skall innehålla.

4 § Personuppgiftsombudet skall hjälpa registrerade att få rättelse när det finns anledning att misstänka att behandlade personuppgifter är felaktiga eller ofullständiga.

5 kap. Tillsynsmyndigheten

1 § Den myndighet som regeringen bestämmer skall utöva tillsyn över Försvarets radioanstalts behandling av personuppgifter enligt denna lag.

2 § Tillsynsmyndigheten har rätt att för sin tillsyn på begäran få

1. tillgång till de personuppgifter som behandlas,
2. upplysningar om och dokumentation av behandlingen av personuppgifter och säkerheten vid denna, och
3. tillträde till sådana lokaler som har anknytning till behandlingen av personuppgifter.

3 § Om tillsynsmyndigheten konstaterar att personuppgifter behandlas eller kan komma att behandlas på ett olagligt sätt, skall myndigheten genom påpekanden eller liknande förfaranden försöka åstadkomma rättelse.

4 § Tillsynsmyndigheten får hos länsrätten i Stockholms län ansöka om att sådana personuppgifter som har behandlats på ett olagligt sätt skall utplånas.
Beslut om utplånande får inte meddelas om det är oskäligt.

6 kap. Övriga bestämmelser

Gallring

1 § Personuppgifter som behandlas automatiserat skall gallras så snart uppgifterna inte längre behövs för det ändamål för vilket de behandlas. Regeringen får dock meddela föreskrifter eller beslut om att gallring skall ske senast vid viss tidpunkt.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om att personuppgifter utan hinder av första stycket får bevaras för historiska, statistiska och vetenskapliga ändamål.

Straff

2 § Till böter eller fängelse i högst sex månader eller, om brottet är grovt, till fängelse i högst två år döms den som uppsåtligen eller av grov oaktsamhet

a) lämnar osann uppgift i sådan information till registrerade som föreskrivs i denna lag, i anmälan till tillsynsmyndigheten enligt 4 kap. 1 § eller till tillsynsmyndigheten när myndigheten begär information enligt 5 kap. 1 § eller

b) behandlar personuppgifter i strid med 1 kap. 10 § .

I ringa fall döms inte till ansvar.

Överklagande

3 § Försvarets radioanstalts beslut om information som skall lämnas enligt 2 kap. 1 § och om rättelse enligt 2 kap. 4 § får överklagas hos allmän förvaltningsdomstol. Andra beslut enligt denna lag får inte överklagas.

Prövningstillstånd krävs vid överklagande till kammarrätten.

1. Denna lag träder i kraft den 1 januari 2007.

2. Bestämmelser i lagen om grundläggande krav på behandling av personuppgifter samt behandling av känsliga personuppgifter skall inte börja tillämpas förrän den 1 oktober 2007 i fråga om sådan manuell behandling av personuppgifter som påbörjats före den 24 oktober 1998 eller manuell behandling som utförs för ett visst bestämt ändamål om manuell behandling för ändamålet påbörjats före den 24 oktober 1998.

2 Ärendet och dess beredning

Regeringen beslutade den 7 februari 2002 att tillkalla en särskild utredare för att göra en översyn av regleringen av behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet. Dåvarande chefen för Försvarsdepartementet förordnade samma dag kammarrättslagmannen Sten Wahlqvist att vara särskild utredare. Utredaren skulle kartlägga behandlingen av personuppgifter och analysera behovet av särskilda bestämmelser i lag (dir. 2002:13). Utgångspunkten var att myndigheternas verksamhet skall kunna bedrivas effektivt med rationellt datorstöd samtidigt som nödvändig respekt visas för enskildas personliga integritet.

Utredningen, som antog namnet Underrättelsedatautredningen, överlämnade i mars 2003 betänkandet Försvarets underrättelseverksamhet och säkerhetstjänst, Integritet – Effektivitet (SOU 2003:34). En sammanfattning av betänkandet finns i *bilaga 1*. Utredningens lagförslag finns i *bilaga 2*. Betänkandet har remissbehandlats. En förteckning över remissinstanserna finns i *bilaga 3*. En sammanställning över remissyttrandena finns tillgänglig i Försvarsdepartementet (dnr Fö2003/991/RS).

I betänkandet föreslogs bl.a. två nya lagar som skall reglera behandlingen av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten respektive Försvarets radioanstalts underrättelseverksamhet. Lagarna föreslogs gälla i stället för personuppgiftslagen, vars bestämmelser tillämpas endast när det anges särskilt. Lagförslagen innehöll

särskilda bestämmelser om Försvarsmaktens och Försvarets radioanstalts databaser.

Under beredningen av underrättelsedatautredningens förslag har det framkommit att det finns behov av en annan lagteknisk lösning. Denna promemoria har därför, med underrättelsedatautredningens betänkande som utgångspunkt, utarbetats inom Regeringskansliet (Försvarsdepartementet). I promemorian läggs fram förslag till en annan lagteknisk reglering av behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst och Försvarets radioanstalts underrättelse- och utvecklingsverksamhet. Syftet med förslagen är att den rättsliga regleringen inte skall förhindra eller försvåra en annars välkommen effektivisering av verksamheten, om det inte är nödvändigt av integritetsskäl. Promemorians bestämmelser är ett resultat av att försöka finna den bästa möjliga avvägning mellan användandet av modern teknik och utveckling av sådan samt skyddet av den enskildes personliga integritet. I denna promemoria (se avsnitt 7.1) föreslås därför bl.a. att de grundläggande principerna för behandling av personuppgifter skall regleras i lag och att kompletterande bestämmelser skall meddelas av regeringen eller den myndighet som regeringen bestämmer. Genom att undvika en detaljreglering på lagnivå hindras inte framtida teknikutveckling och rationaliseringar. De olika register och databaser som används i verksamheterna omnämns därför inte i lagförslagen. Vidare föreslås i promemorian (se avsnitt 7.2) att lagförslagen om behandling av personuppgifter inom dels Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst, dels Försvarets radioanstalts underrättelseverksamhet skall innehålla alla de bestämmelser som skall gälla för behandlingen av personuppgifter inom dessa verksamhetsområden. Lagförslagen är således heltäckande.

Underrättelsedatautredningens betänkande innehöll också ett förslag till en ny bestämmelse om sekretess för uppgift hos Försvarsmakten i den militära underrättelse- och säkerhetstjänsten för uppgift om enskilds personliga eller ekonomiska förhållanden, om det inte står klart att uppgiften kan röjas utan att den

enskilde eller någon närstående till den enskilde lider skada eller men. I fråga om uppgift i allmän handling föreslogs att sekretessen skall gälla i högst sjuttio år. Sekretessfrågan behandlas inte i denna promemoria utan hanteras tillsammans med förslagen i Ds 2005:30 En anpassad försvarsunderrättelseverksamhet, se avsnitt 6.

3 Behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst

3.1 Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst

Försvarmakten är en myndighet under regeringen. De grundläggande uppgifterna för Försvarmakten framgår av bestämmelserna i 1–3 §§ förordningen (2000:555) med instruktion för Försvarmakten. Enligt dessa bestämmelser skall grunden för Försvarmaktens verksamhet vara förmågan till väpnad strid. Försvarmakten skall kunna försvara hela Sverige mot väpnat angrepp var det än kommer ifrån. Försvarmakten skall kunna hävda Sveriges territoriella integritet. Försvarmakten skall bidra till fred och säkerhet i omvärlden genom att kunna genomföra och lämna stöd till fredsfrämjande operationer och säkerhetsfrämjande samarbete samt kunna lämna stöd till humanitär verksamhet. Försvarmakten skall bidra till att stärka det svenska samhället vid svåra påfrestningar i fred genom att kunna samverka med andra myndigheter och kunna ställa resurser till förfogande. Försvarmakten skall ha den operativa förmåga, de kompetenser och den insatsorganisation som regeringen beslutar. Försvarmakten skall även upprätthålla den beredskap som regeringen beslutar. Försvarmaktens beredskap, organisation och planläggning skall medge att Försvarmaktens förmåga kan anpassas för att motsvara förändrade krav och behov. Försvarmakten skall genomföra den planläggning och vidta de förberedelser som behövs för att kunna lösa myndighetens uppgifter.

Försvarmakten skall utöver detta enligt 4 § 1–3 i nämnda instruktion särskilt leda och bedriva försvarsunderrättelseverksamhet och militär säkerhetstjänst samt leda och samordna signalskyddstjänsten inom totalförsvaret. Försvarsunderrättelseverksamhet och militär säkerhetstjänst utövas av den militära underrättelse- och säkerhetstjänsten (MUST), som är en enhet inom Försvarmaktens högkvarter.

Försvarsunderrättelseverksamhet

Försvarsunderrättelseverksamhetens uppgifter och arbetsformer regleras i 1–4 §§ lagen (2000:130) om försvarsunderrättelseverksamhet. Där framgår att försvarsunderrättelseverksamhet skall bedrivas för att kartlägga yttre militära hot mot landet och till stöd för svensk utrikes-, försvars- och säkerhetspolitik. I verksamheten ingår att medverka i svenskt deltagande i internationellt säkerhetssamarbete och att, enligt vad regeringen närmare bestämmer, medverka med underrättelser för att stärka samhället vid svåra påfrestningar på samhället i fred. Med en svår påfrestning avses ett tillstånd som kan uppstå när en eller flera händelser utvecklar sig eller trappas upp till att omfatta flera delar av samhället. Tillståndet är av en sådan omfattning att det uppstår allvarliga störningar i viktiga samhällsfunktioner eller att det hotar grundläggande värden av olika slag i samhället och kräver att insatser från flera olika myndigheter och organ samordnas för att kunna hantera situationen (prop. 2001/02:158 s. 72).

Av lagen framgår vidare att regeringen bestämmer försvarsunderrättelseverksamhetens inriktning. Uppgifterna skall enligt lagen fullgöras genom inhämtning, bearbetning och analys av information. Analyser av hotbilder och bedömningar i underrättelsefrågor skall rapporteras till Regeringskansliet och andra berörda myndigheter. Av lagen framgår att de myndigheter som skall bedriva försvarsunderrättelseverksamhet får, enligt regeringens närmare bestämmande, etablera och upprätthålla samarbe-

te i underrättelsefrågor med andra länder och internationella organisationer. Försvarsunderrättelseverksamheten får inte avse uppgifter som enligt lagar eller andra föreskrifter ligger inom ramen för polisens och andra myndigheters brottsbekämpande och brottsförebyggande arbete.

Försvarsunderrättelseverksamhet skall bedrivas av Försvarsmakten, Försvarets radioanstalt, Totalförsvarets forskningsinstitut och Försvarets materielverk, 1 § lagen och 2 § förordningen (2000:131) om försvarsunderrättelseverksamhet.

Begreppet säkerhetspolitik är en sammanfattande benämning på de åtgärder som ett lands regering vidtar inom ramen för utrikes- och försvarspolitik till skydd mot yttre hot mot landet och för att bevara landets fred och självständighet. Sveriges säkerhetspolitiska mål är att i alla lägen och i former som vi själva väljer trygga en handlingsfrihet att, såsom enskild nation och i samverkan, kunna utveckla vårt samhälle. Den svenska säkerhetspolitikens mål och inriktning blir på så sätt avgörande även för den grundläggande inriktningen av försvarsunderrättelseverksamheten.

De närmare riktlinjerna för verksamheten läggs varje år fast i regeringens regleringsbrev för de fyra försvarsunderrättelsemyndigheterna. Regeringen har i bilaga till regleringsbrevet för Försvarsmakten för budgetåret 2005 angett i huvudsak följande inriktning (se bilaga 3 till regleringsbrevet). Försvarsunderrättelseverksamhet skall bedrivas för att kartlägga yttre militära hot mot landet och till stöd för svensk utrikes-, försvars- och säkerhetspolitik. Försvarsunderrättelsemyndigheterna skall hålla en sådan beredskap att verksamheten snabbt kan anpassas till händelseutvecklingen i omvärlden. Tyngdpunktsförändringen skall fortsätta från traditionell militär, operativ och taktisk förvarning till strategiska och icke-militära underrättelser i linje med den vidgade hotbilden. Till stöd för svensk utrikes-, försvars- och säkerhetspolitik skall försvarsunderrättelsemyndigheterna inhämta och till regeringen löpande rapportera underrättelser i enlighet med vad regeringen beslutat i den särskilda inriktningen. Försvarsunder-

rättelsemyndigheterna skall utveckla sin förmåga att inhämta, analysera och rapportera underrättelser om sådana trender som kan påverka Sverige och som har säkerhetspolitisk relevans. Den vidgade synen på vad som innefattas i hot mot landets säkerhet medför att allt högre krav ställs på försvarsunderrättelsemyndigheterna och deras samverkan med andra myndigheter. Försvarsunderrättelsemyndigheterna skall ge hög prioritet åt sådana underrättelsebehov som uppstår till följd av Sveriges engagemang i olika former av konfliktförebyggande åtgärder samt internationella operationer. Försvarsunderrättelsemyndigheterna skall bidra till ett förstärkt underrättelsesamarbete inom ramen för EU:s gemensamma utrikes- och säkerhetspolitik och EU:s krishanteringsförmåga.

Militär säkerhetstjänst

I säkerhetsskyddslagen (1996:627) finns bestämmelser om säkerhetsskydd. Med säkerhetsskydd avses dels skydd mot spioneri, sabotage och andra brott som kan hota rikets säkerhet, dels skydd i andra fall av uppgifter som omfattas av sekretess enligt sekretesslagen (1980:100) och som rör rikets säkerhet, 6 §. Vidare avses i 6 § med säkerhetsskydd även skydd mot terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott (terrorism), även om brotten inte hotar rikets säkerhet. Med rikets säkerhet avses såväl den yttre säkerheten för det nationella oberoendet som den inre säkerheten för det demokratiska statskicket. Skyddet för den yttre säkerheten tar i första hand sikte på totalförsvaret. Ett hot mot rikets yttre säkerhet kan dock förekomma även om det inte utgör ett hot mot totalförsvaret.

Försvarsmakten, som med stöd av 4 § 2 i förordningen (2000:555) med instruktion för Försvarsmakten skall leda och bedriva militär säkerhetstjänst, måste för att uppfylla syftet med säkerhetsskyddslagen vidta vissa säkerhetsskyddsåtgärder. Dessa åtgärder benämns i lagen informationssäkerhet, tillträdesbe-

gränsning samt säkerhetsprövning. Säkerhetsprövning omfattar ofta registerkontroll och särskild personutredning.

Den militära säkerhetstjänstens uppgift är att upptäcka, identifiera och möta säkerhetsshot som riktas mot Försvarsmakten och dess säkerhetsintressen såväl inom som utom landet. Häri ingår bl.a. att biträda polisen i dess ansvar beträffande skyddet av rikets säkerhet. Försvarsmaktens säkerhetsintressen kan hänföras till personal, materiel, anläggningar, information samt planering och planer i vid bemärkelse.

Den säkerhetsshotande verksamhet som riktas mot Försvarsmakten brukar delas in i underrättelseverksamhet, kriminalitet, sabotage, subversiv verksamhet samt terrorism. Den kan riktas mot hela eller delar av Försvarsmakten, viss funktion eller verksamhet och förband samt verksamhet inom Försvarsmaktens intresseområde, t.ex. försvarsindustri. Underrättelseverksamhet riktad mot Försvarsmakten kan bedrivas av såväl främmande makt som olika organisationer, företag och kriminella personer. Främmande makts underrättelseverksamhet kan ske på svenskt territorium, utanför landet eller riktas mot Försvarsmakten i samband med internationell verksamhet eller uppträdande utomlands i andra sammanhang.

Den militära säkerhetstjänsten omfattar säkerhetsunderrättelsetjänst och säkerhetsskyddstjänst. Säkerhetsunderrättelsetjänsten har till uppgift att klarlägga den säkerhetsshotande verksamhetens omfattning, inriktning samt medel och metoder. Dess syfte är att utifrån aktuella säkerhetsunderrättelsebehov lämna underlag för beslut om t.ex. säkerhetsskyddsåtgärder, beredskap eller förbandsproduktion. Säkerhetsskyddstjänstens uppgift är att ta fram åtgärder som syftar till att hindra eller försvåra säkerhetsshotande verksamhet. Den arbetar med att förebygga att hemliga uppgifter som rör rikets säkerhet obehörigen röjs, ändras eller förstörs. Säkerhetsskyddstjänsten skyddar också materiel och anläggningar mot sabotage och stöld samt personal, anläggningar och materiel mot terrorism. Säkerhetsskyddstjänsten omfattar informationssäkerhet inklusive IT-säkerhet, säkerhets-

prövning, tillträdesbegränsning, utbildning och kontroll av säkerhetsskyddet.

Signalskyddstjänsten, som är en säkerhetsskyddsangelägenhet, syftar till att minska verkan av signalspaning, falsk signalering och störsändning mot totalförsvarets telekommunikations- och IT-system, se 4 § 3 Försvarsmaktens instruktion. Den skall förhindra obehörig insyn i och påverkan på totalförsvarets telekommunikationer samt verka för att sekretessbelagda uppgifter och andra skyddsvärda uppgifter skyddas av kryptografiska funktioner i informationssystem. Skyddet utgörs av text- och trafikskydd. En viktig del av signalskyddstjänsten är kontroll av signalskydd (signalkontroll) i Försvarsmaktens telekommunikations- och informationssystem. Genom signalkontroll klarläggs riskerna för att obehöriga får åtkomst till data eller för att dessa stör eller manipulerar data. Vidare klarläggs genom signalkontroll att systemen används enligt gällande regler. Signalkontroll avser också kontroll av röjande signaler. Med röjande signaler avses oönskade elektromagnetiska eller akustiska signaler som alstras i informationsbehandlande utrustningar och som, om de kan tydas av obehöriga, kan bidra till att information röjs. Resultatet från en signalkontroll utnyttjas i första hand för att förbättra rutinerna vid meddelandeväxling och för att klarlägga vilken information som kan ha kommit obehörig till del i den kontrollerade trafiken.

Enligt regleringsbrevet för budgetåret 2005 för den militära säkerhetstjänsten syftar tjänsten i fred till att tillgodose det långsiktiga säkerhetsskyddet inom Försvarsmakten (se bilaga 4 till regleringsbrevet). Försvarsmakten skall hålla hög beredskap för att snabbt kunna anpassa den militära säkerhetstjänsten till händelseutvecklingen i omvärlden. Samarbete med andra länder och internationella organisationer är en naturlig del av verksamheten och utbyte av information anses nödvändigt för att Sverige skall kunna få del av sådan information som landet behöver men som kräver resurser som saknas.

Enligt 39 § första punkten säkerhetsskyddsförordningen (1996:633) skall Försvarsmakten kontrollera säkerhetsskyddet när det gäller Fortifikationsverket samt de myndigheter som hör till Försvarsdepartementet utom Kustbevakningen, Krisberedskapsmyndigheten, Statens räddningsverk och Styrelsen för psykologiskt försvar. Försvarsmakten kontrollerar således säkerhetsskyddet hos bl.a. Försvarets radioanstalt, Försvarets materielverk och Totalförsvarets forskningsinstitut.

3.2 Den militära underrättelse- och säkerhetstjänstens organisation

Som framgått under avsnitt 3.1, utövas försvarsunderrättelseverksamhet och militär säkerhetstjänst i första hand av den militära underrättelse- och säkerhetstjänsten (MUST), som är en enhet inom Försvarsmaktens högkvarter. Verksamheten leds av chefen för MUST och dennes ställföreträdare. MUST:s verksamhet är sedan den 1 februari 2005 organiserad på bl.a. ett Underrättelsekontor, ett Säkerhetskontor, två avdelningar för ledning och administration samt en speciell enhet för särskild inhämtning av underrättelser.

Ledningsavdelningen hanterar all ingående och utgående information inom MUST. Avdelningen samordnar inriktningen, inhämtningen och delgivningen av underrättelser inom Försvarsmakten. Avdelningen är sammanhållande för MUST:s samverkan med andra länder. Avdelningen samordnar utarbetandet av regelbundna och särskilda rapporteringar om aktuella händelser som påverkar Försvarsmakten eller är av säkerhetspolitiskt eller i övrigt av stort intresse.

Underrättelsekontoret genomför inhämtning, bearbetning och analys samt delgivning av underrättelser rörande säkerhetspolitisk, ekonomisk och militärstrategisk utveckling samt underrättelser om vissa andra länders militära stridskrafter. Underrättelsekontoret utarbetar vidare underlag avseende det militära läget i

konfliktområden där svensk internationell insats är eller kan komma att bli aktuell. Kontoret ansvarar för underrättelser till stöd för svenska förband och enheter som deltar i internationella fredsbevarande och humanitära insatser. Avdelningen inhämtar, bearbetar och delger också underrättelser avseende informationskrigföring, spridning av massförstörelsevapen, terrorism och främmande undervattensverksamhet

Verksamheten utgör stöd för strategisk underrättelsetjänst, operativ verksamhet, försvarsplanering och förbandsproduktion. Avdelningen svarar för produktionen av hotbildsunderlag och fakta beträffande stridskrafter och övrigt stöd.

Underrättelsekontoret utarbetar även underlag för underrättelsesamarbete med andra länder samt lämnar underrättelseunderlag till EU, inom ramen för EU:s konfliktförebyggande och konflikthanterande verksamhet.

Vid en särskild sektion inom Underrättelsekontoret, Sektionen för öppna källor, inhämtas, bearbetas och delges information som är allmänt tillgänglig, bl.a. från internationella databaser via Internet.

Säkerhetskontoret leder under chefen för MUST säkerhetstjänsten inklusive IT-säkerhetsarbetet inom Försvarsmakten och signalskyddsarbetet inom hela Totalförsvaret. Säkerhetskontoret planerar, inhämtar, bearbetar och delger säkerhetsunderrättelser. Säkerhetskontoret har tillsynsansvar för säkerhetstjänsten inom Försvarsmakten och även för vissa andra myndigheter under Försvarsdepartementet (FMV, FHS, FRA, FOI) och Fortifikationsverket. Säkerhetskontoret har tillsynsansvar för signalskyddet i hela Totalförsvaret. Säkerhetskontoret samverkar avseende säkerhetsskydd med Rikspolisstyrelsen och Säkerhetspolisen. Chefen för MUST är Försvarsmaktens säkerhetsskyddschef och chef för Totalförsvarets signalskyddstjänst.

I Säkerhetskontoret ingår den funktion som inom Försvarsmakten och Totalförsvaret kontrollerar teknisk IT-säkerhet och signalskydd och att sekretessbelagd information överförs, lagras och hanteras enbart i därför avsedda system.

Kontoret för särskild inhämtning (KSI) arbetar enbart med inhämtning direkt via enskilda personer, s.k. personbaserad inhämtning. Inhämtat material sammanställs i allmänhet till rapporter som överlämnas för vidare bearbetning inom MUST tillsammans med annat underrättelsematerial.

3.3 Försvarsmaktens informationshantering i den militära underrättelse- och säkerhetstjänsten

3.3.1 Behandling av personuppgifter

Inom MUST behandlas en stor mängd information, däribland personuppgifter. För att Försvarsmaktens verksamhet skall kunna bedrivas effektivt är det av avgörande betydelse att det finns ett rationellt datorstöd. Utifrån de särskilda krav som Försvarsmaktens verksamhet ställer, vad gäller bl.a. informationssäkerhet och sekretess, har det utvecklats olika system för att på automatiserad väg behandla den omfattande mängd uppgifter som är nödvändig för att uppnå syftet med verksamheten.

Uppgifter hämtas in med hjälp av flera olika metoder. Uppgifter samlas huvudsakligen in från olika öppna källor såsom tidskrifter och litteratur samt via Internet. Försvarsattachéerna vid Sveriges olika ambassader är underställda chefen för MUST och även de har till uppgift att hämta in öppen information om bl.a. militärpolitiska förhållanden i värdlandet. Försvarsattachéerna rapporterar också om de säkerhetspolitiska förhållanden i värdlandet som kan få konsekvenser för Sverige. Den underrättelseinformation som attachéerna förmedlar hämtas in genom egna observationer vid möten med utländska kollegor och företrädare för värdlandet samt via öppna källor såsom radio, TV, tidningar och tidskrifter. Inom ramen för Sveriges deltagande i internationella fredsbevarande och humanitära insatser hämtar svenska förbandsenheter in information, som kan vara av betydelse

främst för underrättelseverksamheten och säkerhetsskyddet vid den enskilda operationen. Uppgifter inhämtas även av andra enheter i Försvarmakten. Vidare erhåller MUST information genom de underrättelserapporter som delges av Försvarets radioanstalt.

De uppgifter som hämtas in kan naturligtvis avse såväl personuppgifter som andra uppgifter vilka inte alls kan hänföras till viss person, t.ex. uppgifter om främmande makts stridskrafter. När det gäller personuppgifter förekommer i försvarsunderrättelseverksamheten bl.a. uppgifter om personer som verkar inom andra staters försvars- och underrättelsetjänster och personer som förekommer i underrättelserapporter eller kan komma att få ett underrättelsevärde. I säkerhetstjänsten förekommer uppgifter om t.ex. personer vid andra staters underrättelsetjänster eller annan företrädare för främmande makt som bedöms kunna utgöra ett säkerhetshot, personer som varit föremål för registerkontroll enligt säkerhetsskyddslagen och personer som av annan anledning är av betydelse för den militära säkerhetstjänsten och dess tillsynsområde.

Alla former av behandling av personuppgifter förekommer. Personuppgifter behandlas helt manuellt i särskilda register och i löpande text i olika pappersdokument. Behandling av personuppgifter sker också automatiserat i enskilda handläggares fristående persondatorer samt i elektroniska uppgiftssamlingar där personuppgifterna är gemensamt tillgängliga för flera personer i verksamheten. De manuella register som förs i den militära säkerhetstjänsten är på väg att datoriseras. För att kunna behandla personuppgifter på ett effektivt och ändamålsenligt sätt, anpassat till den stora informationsmängd som är nödvändig för verksamheten, har det inom MUST utarbetats flera olika datorbaserade system.

3.3.2 System för automatiserad behandling av personuppgifter

De olika datoriserade system som används för automatiserad behandling av personuppgifter är individuellt utformade och anpassade till de olika ändamål inom verksamheten som de skall tjäna. De är fysiskt skilda från varandra vilket innebär att uppgifterna inom varje system är åtkomliga endast via vissa särskilda datorer. Anledningen till detta är de stränga säkerhetskrav som föranleds av verksamhetens art och syfte. Endast den särskilda databas som innehåller uppgifter från öppna källor är tillgänglig från handläggarens ordinarie persondator. De olika systemen skiljer sig främst åt när det gäller för vilket eller vilka ändamål uppgifter behandlas i systemet och vilka personer som har tillgång till dessa uppgifter. Varje enskild handläggares persondator är kopplad till en och samma server där den information som är gemensamt tillgänglig finns samlad. Det är av grundläggande betydelse att endast den som är behörig att ta del av vissa uppgifter skall ha möjlighet att göra det.

De system som för närvarande finns för automatiserad behandling av personuppgifter är bl.a. Informationsdatabasen och Informationssystemet för den militära underrättelse- och säkerhetstjänsten (IS UNDSÄK).

Informationsdatabasen

Sektionen för öppna källors övergripande uppgift är att genomföra en militärstrategisk omvärldsbevakning genom att inhämta information via allmänt tillgängliga källor och att sammanställa, bearbeta samt delge sådan information. Sektionen producerar och delger regelbundna sammanställningar över intressanta områden och tar varje dag fram en särskild dygnsrapport som sprids via e-post till Regeringskansliet och andra myndigheter. Sektio-

nen svarar vidare på särskilda underrättelse- eller informationsfrågor från handläggare inom MUST.

Inhämtningen av information från öppna källor sker genom sökning enligt särskilt angiven inriktning. Sökning sker i databaser på Internet och i viss mån i litteratur och tidskrifter m.m. Informationen som samlats in lagras i Informationsdatabasen. I databasen är det möjligt att genom fritextsökning söka efter den information som behövs för att myndigheten skall kunna göra analyser av olika förhållanden i omvärlden.

Det finns inga särskilda behörighetsregler för att ta del av uppgifter i Informationsdatabasen. De handläggare inom Försvarsmakten som har behov av att utnyttja databasen har tillgång till den information som finns där. Uppgifterna i databasen är vidare tillgängliga för andra myndigheter genom direktåtkomst.

Den information i Informationsdatabasen som är av betydelse för MUST kan föras över till Informationssystemet för den militära underrättelse- och säkerhetstjänsten (IS UNDSÄK) och den hanteras där som hemlig.

Informationssystemet för den militära underrättelse- och säkerhetstjänsten (IS UNDSÄK)

Systemet IS UNDSÄK är det största och viktigaste systemet för behandling av personuppgifter inom MUST. Här behandlas merparten av den sekretessbelagda information som är nödvändig för försvarsunderrättelseverksamheten och den militära säkerhetstjänsten.

I IS UNDSÄK behandlas alla typer av uppgifter, såväl personuppgifter som uppgifter som helt saknar anknytning till en fysisk person, t.ex. uppgifter om främmande makts militära förband. I systemet behandlas dels öppen information, dels hemliga uppgifter innefattande uppgifter som är av synnerlig betydelse för rikets säkerhet, d.v.s. så kallat kvalificerat hemliga uppgifter.

Uppgifterna i systemet är endast tillgängliga via vissa särskilda datorenheter och för varje sådan enhet är endast en viss person behörig användare. Behörigheten att ta del av uppgifter är kopplad till vilken befattning den enskilde handläggaren har. Behörigheten är även avgörande för möjligheten att uppdatera och förändra uppgifter i systemet. För varje uppgift eller handling som görs tillgänglig i databasen bestäms vilken behörighet (befattning) som skall gälla för att få ta del av uppgiften samt för att uppdatera eller ändra en uppgift.

IS UNDSÄK tillförs ständigt ny information som bearbetas och analyseras och som därefter utgör underlag för de rapporter och andra åtgärder som är syftet med verksamheten. IS UNDSÄK är även det viktigaste delgivningsinstrumentet när det gäller underrättelser som utarbetas av MUST. Delgivning av underrättelser sker genom att uppgifterna görs tillgängliga för mottagarna inom systemet. Delgivning av underrättelserapporter och annan information med de mottagare som inte har tillgång till IS UNDSÄK sker i första hand i pappersform.

All information som läggs in i IS UNDSÄK indexeras. Detta innebär att alla uppgifter som finns i kommentar- och anteckningsfält samt i bifogade filer i systemet går att söka på genom fritextsökning. Härigenom är det även möjligt att söka på känsliga personuppgifter. Den militära underrättelse- och säkerhetstjänsten har inget självständigt behov av att kunna använda känsliga personuppgifter som sökord. Det kan emellertid i vissa sammanhang vara viktigt att sådana uppgifter kan användas i kombination med andra uppgifter, t.ex. i verksamhet inom ett internationellt fredsbevarande- eller humanitärt projekt som har till syfte att skydda en etnisk minoritet.

Uppgifterna i IS UNDSÄK kan vara av betydelse för den militära underrättelse- och säkerhetstjänsten under lång tid. För ett bra beslutsunderlag krävs att man kan följa personer och företeelser under en mycket lång period. Samtidigt kan uppgifter som i dag inte har direkt betydelse för verksamheten i framtiden visa sig innehålla mycket värdefull information.

4 Behandling av personuppgifter i Försvarets radioanstalts underrättelseverksamhet m.m.

4.1 Försvarets radioanstalts underrättelseverksamhet m.m.

Försvarets radioanstalt är en av de myndigheter som har till uppgift att bedriva försvarsunderrättelseverksamhet. Försvarsunderrättelseverksamhetens uppgifter och arbetsformer samt regeringens inriktning har redovisats i avsnitt 3.1. Det som i detta avseende framförts där om Försvarsmakten är även tillämpligt på Försvarets radioanstalt.

Försvarets radioanstalts verksamhet regleras därutöver i 1 § förordningen (1994:714) med instruktion för Försvarets radioanstalt. Där anges att myndighetens uppgift är att bedriva signalspaning enligt den inriktning som regeringen och andra uppdragsgivare anger. Försvarets radioanstalt är således en uppdragstagande myndighet som skall utföra signalspaning i enlighet med vad olika uppdragsgivare anger såsom målsättning och syfte med signalspaningen.

Försvarets radioanstalts signalspaning innefattar såväl inhämtning som bearbetning och analys samt rapportering till myndighetens olika uppdragsgivare. Signalspaning sker genom att man med mottagarsystem och andra elektroniska hjälpmedel registrerar telesändningar och signaler för att hämta in information som kan användas i underrättelseverksamheten. Signalerna kan komma från kommunikation genom tal, telegrafi, data och fjärrskrift (kommunikationsspaning) eller ha andra funktioner i samband med radar, navigering eller överföring av mätvärden (teknisk sig-

nalspaning). Signalspaning riktar sig mot alla typer av eterburna telesändningar.

Kommunikationsspaningen kan delas in i inhämtning, bearbetning (trafikbearbetning inklusive kryptoforcering och innehållsbearbetning), analys och rapportering. Inhämtning kan ske manuellt genom att en radiooperatör ställer in radiomottagaren tills han eller hon hör något som erfarenhetsmässigt är intressant, eller med hjälp av automatiska spaningssystem. De uppfångade radiosignalerna lägesbestäms, vilket främst sker genom pejling. Trafikbearbetningen syftar till att bringa ordning i det skenbara kaos som det inhämtade materialet erbjuder. Härigenom kan man konstatera vem som kommunicerar med vem och varför. De uppfångade radiosignalerna identifieras och trafikmönster fastställs. Kryptoforceringens yttersta mål är att klargöra den inhämtade informationens faktiska innebörd. För att skydda sig mot detta har krypteringstekniken utvecklats snabbt. På motsvarande sätt har även kryptoforceringen utvecklats och blivit allt mer datorstödd. Kunskap om kryptoforcering är också en nödvändig förutsättning för att kunna konstruera egna goda krypton. Det sista momentet i kommunikationsspaningskedjan är analys och delgivning av det bearbetade underlaget.

Försvarets radioanstalt delger olika underrättelser i enlighet med de riktlinjer som statsmakterna ställer upp. Regeringskansliet är en av mottagarna av underrättelser. Den underrättelseinformation som delges rör huvudsakligen internationella relationer, krishärdar och de internationella uppdrag i vilka svensk personal deltar. Därutöver delges viss information rörande terrorism, exportkontroll, protokollära ärenden och händelser i närheten av svenskt territorium. Myndigheter under Utrikes- respektive Forsvarsdepartementet får underrättelser som hör till respektive myndighets ansvarsområde. Myndigheterna får också information om de internationella uppdrag i vilka svensk personal deltar samt om frågor rörande spridning av massförstörelsevapen, vapenexportärenden och militär teknologisk utveckling.

Den dagliga rapporteringen rör information av betydelse för bedömningar av internationell krishantering samt den allmänna

utrikes- och försvarspolitiska utvecklingen. Regelbunden rapportering sker om bl.a. extremism, terrorism och spridning av massförstörelsevapen. Försvarets radioanstalt rapporterar om förhållandena i vissa regioner som bedöms som kris- eller spänningsområden. En mer långsiktig och bearbetad redovisning sker på månads- eller årsbasis om bland annat underrättelser kopplade till främmande stridskrafter taktik, organisation, struktur och ledning.

Försvarets radioanstalt skall vidare enligt 2 och 3 §§ instruktionen bedriva viss utvecklingsverksamhet. Myndigheten skall således särskilt följa förändringen av signalmiljön i omvärlden, den tekniska utvecklingen och signalskyddet. Myndigheten skall fortlöpande utveckla den teknik och metodik som behövs för att bedriva verksamheten och utföra matematiska bedömningar av kryptosystem för totalförsvaret. Försvarets radioanstalt skall också biträda andra myndigheter vid värdering, utveckling, anskaffning och drift av signalspaningssystem. När teknik utvecklas och när nya metoder för forcering av krypterad information arbetas fram används oftast autentiskt underrättelsematerial för att man skall kunna vara säker på teknikens riktighet. Det autentiska materialet kan innehålla personuppgifter.

Försvarets radioanstalt skall enligt 3 a § första stycket 1–2 instruktionen ha en hög teknisk kompetens inom informationssäkerhetsområdet (jfr. prop. 2001/02:158 s. 109 f). Försvarets radioanstalt får efter begäran stödja sådana statliga myndigheter och statligt ägda bolag (uppdragsgivare) som hanterar information som bedöms vara känslig ur sårbarhetssynpunkt eller ur ett säkerhets- eller försvarspolitiskt avseende. Försvarets radioanstalt skall därvid särskilt kunna stödja insatser vid nationella kriser med IT-inslag och medverka till identifieringen av inblandade aktörer vid IT-relaterade hot mot samhällsviktiga system.

Vidare följer av 3 a § första stycket 3–4 instruktionen att Försvarets radioanstalt får, efter begäran från sådana uppdragsgivare, genomföra IT-säkerhetsanalyser och ge annat tekniskt stöd. Uppdragsgivarna kan ha känsliga datorsystem som de inte vill eller anser sig kunna blottlägga för privata aktörer. De har då

möjlighet att vända sig till Försvarets radioanstalt som på deras begäran kan göra bl.a. en informationssäkerhetsanalys. Informationssäkerhetsanalysen gör det möjligt för uppdragsgivaren att prioritera de insatser som är nödvändiga för att driften av datorsystemen skall kunna säkerställas. Konsultverksamheten på Försvarets radioanstalt har hittills främst rört aktiva IT-kontroller, som innebär att myndigheten på uppdragsgivarens begäran söker efter och analyserar brister i säkerheten i datorsystemen. Den information som Försvarets radioanstalt erhåller i samband med att en aktiv IT-kontroll görs kan innehålla personuppgifter. Vid behandling av dessa personuppgifter agerar Försvarets radioanstalt, med stöd av ett avtal med uppdragsgivaren, som personuppgiftsbiträde för dennes räkning. Personuppgifterna behandlas således av Försvarets radioanstalt helt i enlighet med uppdragsgivarens instruktioner. Den information som Försvarets radioanstalt får i samband med att uppgifterna i 3 a § första stycket 3–4 instruktionen utförs används inte i myndighetens underrättelse- eller utvecklingsverksamhet. Data innehållande bl.a. personuppgifter återsänds till uppdragsgivaren i samband med slutrapport eller förstörs av Försvarets radioanstalt.

Upplivsingsvis kan nämnas att Försvarets radioanstalt enligt 3 a § andra stycket instruktionen skall samverka med andra organisationer inom informationssäkerhetsområdet såväl inom som utom landet.

4.2 Försvarets radioanstalts organisation

Försvarets radioanstalt är en civil myndighet under regeringen. Under generaldirektören finns en stab och åtta avdelningar jämte vissa särskilda funktioner. Med undantag för vad som inryms under en särskild avdelning för teknisk signalspaning har inhämtning, bearbetning respektive analys och rapportering samlats under tre särskilda avdelningar. *Avdelningen för inhämtning* svarar för inhämtning av kommunikationssignaler. Vid avdelningen finns också en enhet som arbetar med undersökning och

utveckling inom telekommunikationsområdet. *Avdelningen för bearbetning* svarar för att inhämtat material bearbetas till information som går att analysera. På avdelningen finns också resurser för kontroll av IT-system. *Avdelningen för underrättelserapportering* analyserar det inhämtade och bearbetade materialet för att sedan producera rapporter som delges uppdragsgivarna. Avdelningen har också en funktion som arbetar med information i öppna källor till stöd för myndighetens arbete.

Avdelningen för teknisk signalspaning genomför egen inhämtning, bearbetning och rapportering.

Vidare finns avdelningar för *systemutveckling, drift och underhåll, personal* och *förvaltning*.

4.3 Försvarets radioanstalts informationshantering i underrättelseverksamheten m.m.

4.3.1 Behandling av personuppgifter i Försvarets radioanstalts underrättelseverksamhet m.m.

Försvarets radioanstalt behandlar i sin underrättelseverksamhet en mycket stor mängd information som inhämtas genom signalspaning och från öppna källor. Informationen som hämtas in i signalspaningsverksamheten är ofta krypterad och avfattad på ett främmande språk. För att Försvarets radioanstalt skall kunna framställa rapporter med underrättelser måste den stora informationsmängden bearbetas och analyseras. För att verksamheten skall kunna bedrivas effektivt behandlas den inhämtade informationen med hjälp av datorer. Enstaka manuella register kan förekomma.

Den information som erhålls genom signalspaning och från öppna källor, såsom t.ex. Internet, kan omfatta allt från det utrikes- och försvarspolitiska området till detaljuppgifter om t.ex. enskilda militära förband eller vapensystem. I underrättelseverksamheten ingår också rapportering av underrättelser som till viss del innehåller personuppgifter. Rapporter kan i viss utsträckning

innehålla uppgifter om personer med relevans för Sverige i utrikes-, försvars- eller säkerhetspolitiskt hänseende.

Försvarets radioanstalt lämnar även ut uppgifter inom ramen för det internationella underrättelsesamarbete som myndigheten deltar i.

4.3.2 System för automatiserad behandling av personuppgifter

De personuppgifter som hämtats in genom signalspaning och från öppna källor lagras i elektronisk form i olika uppgiftssamlingar (databaser). Uppgifterna är sedan gemensamt tillgängliga för flera handläggare inom myndighetens underrättelseverksamhet. De olika uppgiftssamlingarna är inte fysiskt skilda från varandra. De är endast tillgängliga via särskilda datorer. Avgörande för vilken databas en uppgift tillhör är tillvägagångssättet för att ta del av informationen. Tillgång till den information som finns lagrad i de olika uppgiftssamlingarna erhålls via access som är speciell för varje enskild databas. Den underrättelseinformation och andra uppgifter som finns i den enskilda databasen kan handläggaren få tillgång till enligt de särskilda kriterier som gäller för respektive databas, med den begränsning som handläggarens behörighet medger. Tillgången till uppgifter i Försvarets radioanstalts olika databaser är reglerad genom ett särskilt behörighetssystem med ett flertal nivåer. Vilken åtkomst varje enskild handläggare har till uppgifter i de olika databaserna beror på vilka arbetsuppgifter denne har.

Försvarets radioanstalts system för behandling av personuppgifter i underrättelseverksamheten är helt anpassat till underrättelseprocessen. För inriktning av myndighetens underrättelseverksamhet används Urvalsdatabasen. Information som hämtas in lagras i Källdatabasen eller Databasen för öppna källor. Bearbetning och analys sker i Analysdatabasen och underrättelserapporterna som är färdiga för delgivning lagras i Rapportdatabasen.

Urvalsdatan

Urvalsdatan består av en samling uppgifter som används för planering och inriktning av underrättelseverksamheten. Underrättelseverksamheten styrs främst genom riktlinjer och anvisningar från regeringen och Regeringskansliet. Utöver detta bidrar andra uppdragsgivare och samarbetspartners med mer detaljerad information för planering och inriktning av myndighetens underrättelseverksamhet. Informationen som på så sätt kommer in till myndigheten består av meddelanden som tas emot av avdelningen för underrättelserapportering. Avdelningen sammanställer och överför sedan informationen till lämplig uppgiftssamling i myndighetens system av databaser, t.ex. Urvalsdatan.

I Urvalsdatan behandlas främst sökord som kan bestå av olika personuppgifter, t.ex. namn. Den information som lagras i Urvalsdatan används för inriktning på kort och på lång sikt av underrättelseverksamheten. Uppgifterna i databasen används i underrättelseverksamheten vid sökning genom signalspaning och i öppna källor. Spaning sker även efter vissa tekniska parametrar (t.ex. e-postadresser och telefonnummer) vilka även de återfinns i Urvalsdatan.

Källdatabasen

Källdatabasen är den primära databasen för lagring av den information som Försvarets radioanstalt hämtar in i sin underrättelseverksamhet. Källdatabasen innehåller endast hemlig information i form av signalspaningsmaterial.

Inhämtning genom signalspaning kan ske utan urval, vilket innebär att databasen tillförs stora mängder obearbetad information. Källdatabasen är då en ”spegling” av förekommande signaler. Det inhämtade materialet kan vara såväl krypterat som avfattet på ett främmande språk. Försvarets radioanstalt vet således inte på detta stadium i underrättelseprocessen vilken information uppgifterna innehåller.

Försvarets radioanstalt genomför också signalspaning enligt de särskilt utvalda sökkriterier som återfinns i Urvals databasen. Sökning sker då efter dels tekniska parametrar, dels särskilda sökord.

Källdatabasen är en omfattande databas. Till denna förs ständigt nya uppgifter med den konsekvensen att äldre information i princip överlagras när kapacitetstaket nåtts. Lagringstiden varierar starkt. Merparten av data lagras mycket kort tid, men det finns också information som kan behöva lagras under lång tid.

Källdatabasen innehåller, om än till mindre del, personuppgifter som kan eftersökas. Sökorden som används kan då vara t.ex. namn på personer, adresser eller personnummer. I sakens natur ligger att även personuppgifter som rör politiska åsikter, etniskt ursprung och andra känsliga personuppgifter kan förekomma. Behandling av känsliga personuppgifter är en förutsättning för att Försvarets radioanstalt skall kunna utföra sitt uppdrag som leverantör av underrättelser. Sådan känslig information är inte intressant i sig men kan i kombination med andra uppgifter vara av största betydelse för rapporteringen.

Databasen för öppna källor

De uppgifter som samlas in från öppna källor lagras regelmässigt en kort tid i Databasen för öppna källor. I databasen kan myndighetens handläggare i underrättelseverksamheten söka information genom användandet av särskilda sökord. Dessa sökord utgörs antingen av de urvalskriterier som finns i Urvals databasen eller är handläggarens egna. Om uppgifterna bedöms kunna vara av intresse för underrättelseverksamheten förs uppgifterna över till Analysdatabasen för vidare bearbetning och analys.

Databasen för öppna källor innehåller personuppgifter avseende framför allt utländska men även svenska medborgare samt uppgifter med anknytning till vissa personer. Detta är i stor utsträckning samma uppgifter som återfinns i Urvals databasen i form av sökord och andra urvalskriterier. Personuppgifterna an-

vänds som sökord och fungerar således som ingång till andra uppgifter om personer som är intressanta i underrättelseverksamheten.

Varje dag inhämtas ett mycket stort antal personuppgifter från öppna källor. Det är emellertid endast en bråkdel av denna information som sparas för vidare bearbetning innan informationen, på grund av att kapacitetstaket i databasen nåtts, överlagras av ny information och på så sätt försvinner. Det är vidare ytterst få av de uppgifter som lagras i databasen som är att betrakta som känsliga i personuppgiftslagens mening.

Analysdatabasen

I Analysdatabasen sker bearbetning, såsom dekryptering och översättning, av den information som hämtats in och lagrats i Källdatabasen och Databasen för öppna källor. Bearbetningen går ut på att göra materialet läsbart och hanterbart för analys, vilket också sker i Analysdatabasen sedan informationen bearbetats. I Analysdatabasen mellanlagras också arbetsmaterialet innan det färdigställs till underrättelserapporter och lagras i Rapportdatabasen. I Analysdatabasen görs bedömningen av om Försvarets radioanstalt skall arbeta vidare med materialet eller om det skall sällas bort.

I databasen behandlas både hemlig och öppen information. Den öppna information som bedöms vara av intresse för underrättelseverksamheten överförs från Databasen för öppna källor till Analysdatabasen, men ursprunget blir tydligt spårbart.

Rapportdatabasen

Rapportdatabasen innehåller endast underrättelserapporter. Av varje rapport framgår det ämne rapporten behandlar och den uppdragsgivare som skall ha rapporten. Rapporter kan eftersökas

i databasen genom användande av namn på uppdragsgivare, datum på rapporten eller det ämne rapporten behandlar.

I de slutliga underrättelserapporterna har all ovidkommande information sållats bort. I rapporterna presenteras enbart det som bedöms vara väsentligt för uppdragsgivarna.

Rapporterna kan delges myndighetens uppdragsgivare och andra behöriga mottagare via datorsamband. Av sekretesskäl delges dock huvuddelen av rapporterna i pappersform.

5 Gällande rätt

5.1 Övergripande rättslig reglering av behandling av personuppgifter

5.1.1 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 gäller som lag i Sverige. Artikel 8 i konventionen har betydelse för myndigheternas rätt att behandla personuppgifter. I artikeln stadgas att var och en har rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. En offentlig myndighet får inte inskränka denna rättighet annat än med stöd av lag. Som ytterligare förutsättning gäller att den inskränkande åtgärden skall vara nödvändig i ett demokratiskt samhälle 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.

När det gäller laglighetskriteriet krävs att den inskränkande åtgärden grundas på nationell lag och att den åberopade lagen uppfyller vissa minimikrav i fråga om kvalitet och tydlighet. En rättighetsinskränkande tolkning av lagen skall kunna förutses och lagen skall vara allmänt tillgänglig. Europadomstolen avgör vad som kan anses nödvändigt för att tillgodose ett i och för sig legitimt syfte. En inskränkande åtgärd bedöms nödvändig endast om den svarar mot ett mycket angeläget behov och om den står i rimlig proportion till det syfte som skall uppnås.

I artikel 13 föreskrivs att var och en som anser sig ha fått sina fri- och rättigheter kränkta skall ha tillgång till ett effektivt rättsmedel inför en nationell myndighet. Detta gäller enligt artikeln även om kränkningen förövats av någon under utövning av offentlig myndighet. Prövningen kan utföras av domstol, men även prövning av en stats regering eller av en förvaltningsmyndighet kan vara tillräcklig.

5.1.2 Dataskyddskonventionen

Bestämmelser av betydelse för automatisk databehandling av personuppgifter finns i bl.a. Europarådets konvention från 1981 om skydd för enskilda vid automatisk databehandling av personuppgifter (dataskyddskonventionen). Dataskyddskonventionen trädde i kraft den 1 oktober 1985. Samtliga medlemsstater i EU har ratificerat konventionen. Konventionen är alltså bindande för medlemsstaterna, däribland Sverige.

Dataskyddskonventionens innehåll kan ses som en precisering av skyddet för enskilda vid användning av automatisk databehandling enligt artikel 8 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna. Dataskyddskonventionens syfte är att säkerställa den enskildes rätt till personlig integritet i samband med behandling av personuppgifter och att förbättra förutsättningarna för ett fritt informationsflöde över gränserna.

Dataskyddskonventionen innehåller principer för dataskydd som de konventionsanslutna staterna måste uppfylla i sin nationella lagstiftning. Personuppgifter som är föremål för automatisk databehandling skall hämtas in och behandlas på ett korrekt sätt för särskilt angivna ändamål. Uppgifterna måste vara relevanta för ändamålen och får inte senare användas på ett sätt som är oförenligt med dessa. Vidare måste uppgifterna vara riktiga och aktuella och uppgifterna får inte bevaras längre än vad som är nödvändigt för ändamålen.

Vissa typer av personuppgifter får behandlas endast om den nationella lagen ger ett ändamålsenligt skydd. Till sådana per-

sonuppgifter hör uppgifter om ras, politisk tillhörighet, religiös tro eller övertygelse i övrigt, hälsa, sexualliv samt brott.

För att skydda personuppgifter mot oavsiktlig eller otillåten förstörelse m.m. föreskriver konventionen att lämpliga skyddsåtgärder skall vidtas. Vidare skall den registrerade ha möjligheter till insyn i register och till att få uppgifter rättade. I vissa fall får undantag göras från bestämmelserna om uppgifternas beskaffenhet och rätten till insyn. Sådana inskränkningar i den enskildes skydd förutsätter stöd i den nationella lagstiftningen och att inskränkningen är nödvändig i ett demokratiskt samhälle för vissa ändamål, t.ex. statens penningintressen och brottsbekämpning samt för att skydda enskildas fri- och rättigheter.

Dataskyddskonventionens roll som riktmärke för automatiserad behandling av personuppgifter inom Europeiska unionen har i princip övertagits av 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). Data-skyddsdirektivet omfattar dock inte behandling av personuppgifter inom områden som t.ex. allmän säkerhet, försvar och statens säkerhet. På dessa områden är dataskyddskonventionen således fortfarande av betydelse.

Europarådets ministerkommitté har under 2001 antagit ett tilläggsprotokoll till dataskyddskonventionen. Det innehåller bestämmelser om tillsynsmyndigheter och överföring av personuppgifter till länder som inte är bundna av konventionen. Sverige undertecknade och ratificerade tilläggsprotokollet den 8 november 2001. Tilläggsprotokollet trädde i kraft den 1 juli 2004.

5.1.3 Personuppgiftslagen

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) syftar till att garantera en hög och i alla medlemsstater likvärdig skyddsnivå när det gäller en-

skilda personers fri- och rättigheter med avseende på behandling av personuppgifter och främja ett fritt flöde av personuppgifter mellan medlemsstaterna. Direktivet gäller inte, som framgått, för sådan behandling av personuppgifter som rör allmän säkerhet, försvar, statens säkerhet och statens verksamhet på straffrättsens område. Behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet omfattas således inte av direktivet. Personuppgiftslagen (1998:204), genom vilken direktivet införlivas i svensk rätt, har däremot gjorts generellt tillämplig och omfattar även sådan verksamhet som faller utanför direktivets tillämpningsområde.

Personuppgiftslagen innehåller den grundläggande ramen för behandling av personuppgifter. Särreglering i lag eller förordning gäller framför bestämmelserna i personuppgiftslagen, 2 §. Att det krävs en särskild författning för att avvika från det integritetsskydd som personuppgiftslagen ger är en garanti för att behovet av särregler övervägs noga i den ordning som gäller för författningsgivning. Målet har också varit att myndighetsregister med ett stort antal registrerade och ett särskilt känsligt innehåll skall regleras särskilt i lag (jfr. bet. 1990/91:KU11 s. 11 och 1997/98:KU18 s. 48 samt prop. 1990/91:60 s. 58 och prop. 1997/98:44 s. 40f.).

Behandling av personuppgifter som inte sker med stöd av personuppgiftslagen är otillåten. Med behandling av personuppgifter avses varje åtgärd som vidtas med uppgifterna. Personuppgifter är all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet, 3 §. Uppgifter om juridiska personer och avlidna omfattas således inte av lagen.

Personuppgiftslagen gäller för all automatiserad behandling av personuppgifter. Lagen är dessutom tillämplig på manuell behandling av uppgifter som ingår, eller är avsedda att ingå, i en strukturerad samling av personuppgifter, vilka är tillgängliga för sökning eller sammanställning enligt särskilda kriterier, 5 §.

Den personuppgiftsansvarige är ansvarig för behandling av personuppgifter och skall bl.a. se till att behandlingen av dessa

uppfyller vissa grundläggande krav, såsom t.ex. att behandlingen är laglig, 9 §.

Enligt personuppgiftslagen är det tillåtet att behandla personuppgifter om den registrerade har lämnat sitt samtycke till behandlingen. Personuppgifter får – när samtycke från den registrerade saknas – behandlas om det är nödvändigt bl.a. för att ett avtal med den registrerade skall kunna fullgöras, för att den personuppgiftsansvarige skall kunna fullgöra en rättslig skyldighet eller för att en arbetsuppgift av allmänt intresse skall kunna utföras, 10 §.

Känsliga personuppgifter som t.ex. uppgifter om ras eller etniskt ursprung, politiska åsikter, hälsa eller sexualliv får inte behandlas, 13 §. Känsliga personuppgifter får dock behandlas bl.a. när den registrerade har lämnat sitt uttryckliga samtycke till behandling eller när den registrerade har offentliggjort känsliga uppgifter på ett tydligt sätt, 15–16 §§.

Det är förbjudet enligt personuppgiftslagen för andra än myndigheter att behandla personuppgifter om lagöverträdelse, domar och säkerhetsåtgärder i brottmål, 21 §. Uppgifter om personnummer och samordningsnummer får behandlas bara när den registrerade samtycker till det eller när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl, 22 §.

När uppgifter samlas in från den registrerade själv eller från en annan källa skall den personuppgiftsansvarige självständigt lämna den registrerade viss i lagen angiven information rörande behandling av personuppgifter. Informationen skall bl.a. omfatta uppgifter om ändamålet med behandlingen. Den personuppgiftsansvarige är vidare skyldig att, efter ansökan, en gång per kalenderår gratis informera om huruvida uppgifter som rör sökanden behandlas eller inte m.m. Bestämmelserna om informationsskyldighet gäller inte om sekretess eller tystnadsplikt för uppgifterna är föreskriven i förhållande till den registrerade, 23–27 §§.

Personuppgifter som är felaktiga eller ofullständiga eller som annars inte har behandlats i enlighet med personuppgiftslagen eller anknytande föreskrifter skall på begäran av den registrerade

rättas, utplånas eller blockeras av den personuppgiftsansvarige, 28 §.

Den personuppgiftsansvarige har enligt personuppgiftslagen ett ansvar för säkerheten vid behandling av personuppgifter och för att tekniska och organisatoriska åtgärder vidtagits för att skydda de behandlade personuppgifterna, 30–31 §§.

Det är enligt personuppgiftslagen förbjudet att utan samtycke från den registrerade föra över personuppgifter till en stat utanför EU eller EES som inte har en adekvat nivå för skyddet av personuppgifter. Från överföringsförbudet görs vissa undantag, 33–35 §§.

Enligt dataskyddsdirektivet skall en eller flera tillsynsmyndigheter utses. I Sverige har bl.a. Datainspektionen tilldelats den uppgiften. Som ett led i sin tillsynsverksamhet skall Datainspektionen ha tillgång till behandlade personuppgifter och dessutom tillträde till lokaler med anknytning till behandlingen, 43 §.

Den personuppgiftsansvarige skall anmäla helt eller delvis automatiserad behandling av personuppgifter till Datainspektionen. Anmälan behöver inte göras när ett personuppgiftsombud har utsetts av den personuppgiftsansvarige. Personuppgiftsombudet skall ha till uppgift att självständigt se till att den personuppgiftsansvarige behandlar personuppgifter på ett lagligt och korrekt sätt och i enlighet med god sed, 36–40 §§.

Den personuppgiftsansvarige skall ersätta den registrerade för skada och kränkning av den personliga integriteten som en behandling av personuppgifter i strid med personuppgiftslagen har orsakat, 48 §.

Bestämmelserna i personuppgiftslagen redovisas närmare i samband med de förslag som lämnas i avsnitt 8 och 9.

5.2 Rättslig reglering av behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst samt Försvarets radioanstalts underrättelseverksamhet

5.2.1 Gemensamma bestämmelser

Den behandling av personuppgifter som omfattas av denna promemoria regleras i dag i förordningen (2001:703) om viss behandling av personuppgifter inom Försvarmakten och Försvarets radioanstalt. I förordningen finns dels allmänna bestämmelser som gäller för behandling av personuppgifter både i Försvarmaktens och i Försvarets radioanstalts verksamhet, dels särskilda bestämmelser som gäller enbart för Försvarmaktens respektive Försvarets radioanstalts behandling av personuppgifter.

Förordningen gäller utöver personuppgiftslagen (1998:204) i fråga om viss behandling inom Försvarmakten och Försvarets radioanstalt om behandlingen är helt eller delvis automatiserad, 1 §. Detta innebär att personuppgiftslagens regler är tillämpliga i den mån det inte finns avvikande bestämmelser i den särskilda förordningen.

Förordningen gäller dels för Försvarmakten när myndigheten fullgör uppgifter enligt lagen (2000:130) om försvarsunderrättelseverksamhet, den därtill hörande förordningen och säkerhetskyddslagen (1996:627), dels för Försvarets radioanstalt när myndigheten fullgör uppgifter enligt lagen och förordningen om försvarsunderrättelseverksamhet samt enligt 1–3 §§ förordningen (1994:714) med instruktion för Försvarets radioanstalt, 2 §.

Känsliga personuppgifter får enligt förordningen inte utgöra ensam grund för behandling. Behandlas uppgifter om en person på annan grund får uppgifterna dock kompletteras med sådana känsliga personuppgifter, om det är nödvändigt för syftet med behandlingen, 4 §.

Uppgifter får lämnas ut till en utländsk myndighet eller en internationell organisation endast om utlämnandet tjänar den

svenska statsledningen eller det svenska totalförsvaret och inte är till skada för svenska intressen, 5 §.

I fråga om rättelse och skadestånd anges i 6 § att bestämmelserna i personuppgiftslagen gäller. Personuppgifter som behandlats enligt förordningen skall gallras senast tio år efter den senaste införda uppgiften om den registrerade. Om det finns särskilda skäl får dock uppgifterna stå kvar under längre tid. Riksarkivet får, efter samråd med Försvarmakten eller Försvarets radioanstalt, meddela föreskrifter om att uppgifter som skall gallras får bevaras för historiska, statistiska eller vetenskapliga ändamål, 16 §.

5.2.2 Särskilda bestämmelser för Försvarmaktens behandling av personuppgifter

Försvarmakten skall föra försvarsunderrättelseregister. Ett försvarsunderrättelseregister har till särskilt ändamål att underlätta tillgången till allmänna uppgifter med anknytning till försvarsunderrättelseverksamhet samt att ge underlag för säkerhetspolitiska och militärstrategiska bedömningar, analys av pågående och bedömda framtida konflikter samt biografisk försvarsunderrättelsetjänst, 7 §.

Förvarsunderrättelseregister får endast innehålla personuppgifter om det är nödvändigt för att Försvarmakten skall kunna fullgöra sina uppgifter enligt lagen och förordningen om försvarsunderrättelseverksamhet. Förvarsunderrättelseregister får endast innehålla identifieringsuppgifter, uppgifter om de omständigheter och händelser som ger anledning att anta att den registrerade har betydelse för försvarsunderrättelseverksamheten, och upplysningar om varifrån den registrerade uppgiften kommer och om uppgiftslämnarens trovärdighet, 8–9 §§.

Försvarmakten skall föra säkerhetsregister, i den omfattning som är nödvändig, för att kunna bedriva säkerhetsknyddsvksamhet. Ändamålet med sådan behandling är att ge underlag för beslut eller bedömningar i frågor som syftar till att förhindra säkerhetshotande verksamhet som riktas mot Försvarmakten,

andra myndigheter eller någon annan som Försvarsmakten enligt säkerhetsskyddsförordningen (1996:633) har tillsyn över, 13 §.

Ett säkerhetsregister får endast innehålla personuppgifter

– om personen kan misstänkas för att ha utövat eller komma att utöva verksamhet som innefattar hot mot rikets säkerhet eller terrorism,

– om uppgifter förekommer i samband med att en person har genomgått registerkontroll enligt säkerhetsskyddslagen,

– om det kan antas att personen bedriver annan säkerhetshotande verksamhet och det finns särskilda skäl till att registret skall innehålla uppgiften eller

– om personen har lämnat uppgifter om säkerhetshotande verksamhet. Det skall av registret framgå på vilken grund registrering skett, 14 §.

Ett säkerhetsregister får endast innehålla identifieringsuppgifter, uppgifter om de omständigheter och händelser som ger anledning att anta att den registrerade har betydelse för myndighetens verksamhet att förhindra säkerhetshotande verksamhet, upplysningar om varifrån den registrerade uppgiften kommer och om uppgiftslämnarens trovärdighet, och hänvisning till de ärenden där uppgifter om den registrerade behandlas, 15 §.

5.2.3 Särskilda bestämmelser för Försvarets radioanstalts behandling av personuppgifter

Försvarets radioanstalt skall, enligt förordningen, ha följande databaser; källdatabas, styrdatabas, analysdatabas och underrättelsedatabas. Databaserna har enligt förordningen till ändamål att möjliggöra den bearbetning av information som behövs för att myndigheten skall kunna fullgöra sina uppgifter. Databaserna får innehålla personuppgifter endast om det är nödvändigt för att Försvarets radioanstalt skall kunna fullgöra sina uppgifter enligt lagen och förordningen om försvarsunderrättelseverksamhet och myndighetens instruktion, 10–11 §§.

En källdatabas får endast innehålla obearbetat och automatiskt bearbetat material inhämtat genom signalspaning och från öppna

källor. En styrdatabas får endast innehålla långsiktiga inhämtningsdirektiv eller kortsiktig spaningsinriktning. En analysdatabas får endast innehålla analysresultat samt bearbetnings- och rapportunderlag, och en underrättelsesdatabas får endast innehålla färdiga rapporter, 12 §.

6 Sammanfattning av förslagen i Ds 2005:30 En anpassad försvarsunderrättelse- verksamhet

6.1 Förslag som rör försvarsunderrättelseverksamheten

Mot bakgrund av den allt mer komplexa säkerhetspolitiska hotbilden, den tekniska utvecklingen och det ökade svenska engagemanget i internationella insatser föreslås i promemorian vissa ändringar i lagen (2000:130) om försvarsunderrättelseverksamhet. Försvarsunderrättelseverksamheten skall enligt förslaget bedrivas till stöd för svensk utrikes-, säkerhets- och försvarspolitik samt i övrigt för kartläggning av yttre hot mot landet. I verksamheten skall också ingå att medverka i svenskt deltagande i internationellt säkerhetssamarbete.

Förslaget innebär att försvarsunderrättelseverksamheten kan användas för att möta en bredare hotbild än tidigare, då mandatet varit begränsat till ”yttre militära hot”. Genom ändringen ges förutsättningar för att utnyttja försvarsunderrättelsemyndigheternas resurser också i fråga om t.ex. terrorism, storskalig internationell kriminalitet och kvalificerade IT-relaterade hot.

Försvarsunderrättelseverksamhet skall även fortsättningsvis endast få avse utländska förhållanden, dvs. verksamheter eller företeelser som har sin utgångspunkt i utlandet. Försvarsunderrättelseverksamheten skall följaktligen inhämta, bearbeta och delge sådan information om företeelser och förhållanden i andra länder som bl.a. ger svenska säkerhetspolitiska beslutsfattare ett förbättrat underlag för beslut och bedömningar i utrikes-, säkerhets- och försvarspolitiska frågor eller att skydda svensk personal som deltar i internationella insatser.

Det utvidgade mandatet för försvarsunderrättelseverksamheten aktualiserar frågan om gränsdragningen mellan försvarsunderrättelseverksamhet och polisiär verksamhet. I denna del föreslås i promemorian att den befintliga bestämmelsen förtydligas så att det framgår att försvarsunderrättelseverksamhet inte får innefatta åtgärder som ligger inom ramen för polisens och andra myndigheters brottsbekämpande och brottsförebyggande verksamhet enligt lagar och förordningar. Detta skall dock inte gälla när försvarsunderrättelseverksamheten, utan att riktas mot fysisk person, bedrivs för kartläggning av utländska förhållanden som innebär yttre hot mot landet.

Liksom hittills skall regeringen bestämma försvarsunderrättelseverksamhetens inriktning. Enligt promemorians förslag skall det av lagen framgå att också de myndigheter som har behov av försvarsunderrättelser skall kunna ge närmare inriktning av verksamheten, inom den ram som regeringen fastställt.

Försvarsunderrättelseverksamhet skall även fortsättningsvis bedrivas av Försvarsmakten, Försvarets radioanstalt, Försvarets materielverk och Totalförsvarets forskningsinstitut.

I promemorian föreslås en mindre ändring i fråga om regleringen av rapportering av underrättelser. Förslaget innebär ett tydliggörande av att det som skall rapporteras från försvarsunderrättelsemyndigheterna är resultatet av den process som innefattar inhämtning, bearbetning och analys. Obearbetat råmaterial är följaktligen inte att betrakta som en underrättelse och skall inte rapporteras. Den analys materialet skall genomgå före rapportering skall vara av grundläggande karaktär. Den slutliga bedömningen av materialet skall ske hos mottagaren, dvs. i Regeringskansliet och hos sakansvariga myndigheter.

Underrättelserna skall i huvudsak grunda sig på teknisk och personbaserad inhämtning med särskilda metoder. Sådana metoder används endast av Försvarsmakten och Försvarets radioanstalt. Det föreslås ingen närmare precisering i lagen om försvarsunderrättelseverksamhet av vad dessa metoder innefattar. I fråga om teknisk inhämtning genom signalspaning föreslås en särskild lag, se nedan.

Försvarets underrättelsenämnd är det organ som har till uppgift att följa verksamheten inom de myndigheter som utövar försvarsunderrättelseverksamhet. När mandatet för försvarsunderrättelseverksamhet utökas finns anledning att ytterligare betona betydelsen av en utomstående granskning av dessa myndigheters verksamhet. I promemorian föreslås därför att Försvarets underrättelsenämnd skall ha till uppgift att kontrollera försvarsunderrättelseverksamheten hos de myndigheter som bedriver sådan verksamhet. Nämnden tillförs också ytterligare uppgifter genom den reglering av signalspaningsverksamheten som beskrivs nedan.

Med den organisation Försvarets underrättelsenämnd har i dag är förutsättningarna för en sådan utökad kontrollfunktion som föreslås begränsade. Nämnden skall därför enligt förslaget utökas med en ledamot och förstärkas med ett permanent kansli under ledning av en kanslichef.

6.2 Förslag till lag om signalspaning

I dagsläget bedriver Försvarets radioanstalt signalspaning i etern. Någon särskild lagreglering av den verksamheten finns inte. Mot bakgrund av den tekniska utvecklingen, som bl. a. innebär att allt mer kommunikation förmedlas i tråd, föreslås att signalspaningsmandatet utvidgas till att också omfatta signaler i tråd. Eftersom signalspaning mot kommunikationer kan innebära intrång i det skydd för enskildas integritet som uppställs i regeringsformen och Europakonventionen, föreslås en lagreglering av verksamheten. Den föreslagna lagen ger tydliga ramar för under vilka förutsättningar signalspaning får bedrivas och innehåller mekanismer till skydd för enskildas integritet.

Enligt förslaget till lag om signalspaning skall signaler i elektronisk form få inhämtas för den verksamhet som anges i lagen (2000:130) om försvarsunderrättelseverksamhet. Sådan inhämtning skall också få ske för att följa förändringen i signalmiljön i omvärlden, den tekniska utvecklingen och signalskyddet, samt

för att fortlöpande utveckla den teknik och metodik som behövs för att bedriva signalspaningsverksamheten. Den tekniskt orienterade verksamhet som inte inryms under begreppet försvarsunderrättelseverksamhet syftar till att upprätthålla kompetensen hos signalspaningsmyndigheten för att därigenom möjliggöra försvarsunderrättelseproduktion för regeringen och myndigheters behov. Signalspaning enligt lagen skall bedrivas av Försvarets radioanstalt.

Lagstiftningen föreslås reglera inhämtning av signaler i elektronisk form oavsett om de förmedlas i etern eller i tråd. Inhämtning av signaler i tråd skall endast få avse sådana signaler som förs över Sveriges gräns.

Den trafik som förmedlas genom signaler i elektronisk form är oerhört omfattande. Endast en mycket liten del är av intresse ur försvarsunderrättelsesynpunkt. För att hitta den relevanta informationen måste inhämtningen av signaler i stor utsträckning ske automatiserat med hjälp av sökbegrepp som identifierar de signaler som är av intresse. Enligt förslaget skall all inhämtning i tråd ske automatiserat med hjälp av sökbegrepp, och sådana sökbegrepp skall också användas vid automatiserad inhämtning av signaler i etern. Det föreslås vidare en särskild begränsning när det gäller användning av sökbegrepp som är direkt hänförliga till viss fysisk person; sådana skall endast få användas om det är av synnerlig vikt för verksamheten.

I likhet med vad som gäller för övrig försvarsunderrättelseverksamhet inriktas också signalspaningen av regeringen, och de myndigheter som regeringen bestämmer får möjlighet att inom ramen för regeringens inriktning närmare inrikta verksamheten. Eftersom signalspaning kan innebära intrång i enskildas integritet föreslås att annan myndighet än Regeringskansliet inte skall få inrikta verksamheten utan tillstånd. Sådant tillstånd skall lämnas av Försvarets underrättelsenämnd. Nämnden skall därvid kontrollera att en myndighets inriktning avser inhämtning som är förenlig med de ändamål för vilka försvarsunderrättelseverksamheten får bedrivas och att inriktningen inte endast avser viss fysisk person.

För att säkerställa att information inhämtad genom signalspanning inte används för andra syften än de som anges i lagen föreslås att upptagning eller uppteckning av uppgifter av signaler i elektronisk form omgående skall förstöras om den bl.a. bedömts sakna betydelse för den verksamhet som regleras i lagen. I samma syfte föreslås att rapportering av underrättelser som baseras på information inhämtad genom signalspanning endast skall få avse förhållanden som är av betydelse för ändamålet med verksamheten såsom den formulerats i 1 § lagen (2000:130) om försvarsunderrättelseverksamhet.

Försvarets underrättelsenämnd skall kontrollera efterlevnaden av lagen om signalspanning. I kontrollen skall särskilt ingå en granskning av sökbegreppen och av rapporteringen.

För att Försvarets radioanstalt skall få tillgång till signaler som förmedlas i tråd föreslås en bestämmelse i lagen (2003:389) om elektronisk kommunikation med innebörden att trådgående operatörer skall överföra all trafik som förs över Sveriges gräns till särskilda samverkanspunkter.

7 Allmänna utgångspunkter

7.1 Särskild författningsreglering

Förslag: Behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst samt Försvarets radioanstalts underrättelse- och utvecklingsverksamhet skall författningsregleras särskilt.

De grundläggande principerna för behandling av personuppgifter skall regleras i lag. Kompletterande bestämmelser skall meddelas av regeringen eller den myndighet som regeringen bestämmer.

Utredningens förslag överensstämmer i princip med promemorians.

Remissinstanserna tillstyrker eller har inget att invända mot en särskild författningsreglering eller utformningen av lagstiftningen.

Skäl för förslaget: Personuppgiftslagen innehåller allmänna bestämmelser om integritetsskydd vid behandling av personuppgifter. Det går dock inte att generellt lösa alla problem och fullt ut beakta alla frågeställningar genom att vända sig till personuppgiftslagens bestämmelser. Det behövs ofta en särskild författningsreglering för att anpassa och förstärka integritetsskyddet på särskilda områden. En förutsättning är att en sådan reglering står i överensstämmelse med dataskyddsdirektivet när detta är tillämpligt. Som framgått av avsnitt 5 omfattar inte dataskyddsdirektivets bestämmelser behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och militära

säkerhetstjänst och Försvarets radioanstalts underrättelse- och utvecklingsverksamhet. Utgångspunkten är naturligtvis ändå att författningsförslagen i denna promemoria inte skall strida mot de grundläggande och bindande principerna i dataskyddsdirektivet, även om det skulle vara EG-rättsligt möjligt.

Inom Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst samt i Försvarets radioanstalts underrättelse- och utvecklingsverksamhet är det nödvändigt med en särskild författningsreglering av personuppgiftsbehandlingen av såväl effektivitets- som integritetsskäl. Omfattningen av verksamheterna, deras speciella inriktning samt den stora mängden uppgifter av ofta känslig natur och behandlingar som förekommer talar för en särskild författningsreglering. Det är för allmänhetens förtroende för Försvarmakten och Försvarets radioanstalt och de nu aktuella verksamheterna, vilka av naturliga skäl till största delen är sekretessbelagda, viktigt med en hög nivå på integritetsskyddet.

Försvarsunderrättelseverksamhet bedrivs också av Försvarets materielverk och Totalförsvarets forskningsinstitut. Karaktären, inriktningen och omfattningen av dessa myndigheters verksamhet skiljer sig dock från den som bedrivs av Försvarmakten och Försvarets radioanstalt, särskilt i fråga om behandling av känsliga personuppgifter. Någon författningsreglering av personuppgiftsbehandling motsvarande den som nu föreslås för Försvarmakten och Försvarets radioanstalt är därför inte nödvändig för den försvarsunderrättelseverksamhet som bedrivs av Försvarets materielverk och Totalförsvarets forskningsinstitut. Det är däremot självklart att i den utsträckning behandling av personuppgifter äger rum inom ramen för denna försvarsunderrättelseverksamhet, skall behandlingen inte få ske i vidare mån än som framgår av de föreslagna lagarna. Detta behöver dock inte anges i lag utan kan regleras på annat sätt.

Frågan är i vilken form en särskild författningsreglering skall ske av personuppgiftsbehandlingen i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst samt i Försvarets radioanstalts underrättelse- och utvecklingsverksamhet.

Frågor om regleringen av personregister har behandlats av konstitutionsutskottet, som bl.a. påpekat att myndighetsregister med ett stort antal registrerade och ett känsligt innehåll skall regleras särskilt i lag (bet. 1990/91:KU11 s. 11 och 1997/98:KU18 s. 48). Detta är en uppfattning som även regeringen har gett uttryck för (se bl.a. prop. 1990/91:60 s. 58 och 1997/98:44 s. 41).

Den automatiserade behandling av personuppgifter som förekommer i den militära underrättelse- och säkerhetstjänstens samt Försvarets radioanstalts verksamheter är av sådan karaktär och omfattning att de grundläggande principerna för behandlingen skall slås fast i lag. Vid utformningen av lagstiftningen måste hänsyn tas till att verksamheterna vid de båda myndigheterna är av grundläggande betydelse för Sveriges oberoende och yttre säkerhet. Sådan lagstiftning måste därför vara övergripande och utformad på ett sådant sätt att verksamheterna kan bedrivas effektivt samtidigt som en hög nivå på integritetsskyddet uppnås. Det är av naturliga skäl inte möjligt eller lämpligt att i lagform reglera den personuppgiftsbehandling som sker i verksamheterna i detalj (jfr. prop. 1999/2000:25 s. 12).

De bestämmelser som måste framgå av lag är främst sådana som anger för vilka ändamål personuppgifter får behandlas, vilka typer av uppgifter som får behandlas, i vilken omfattning uppgifter skall få lämnas ut i elektronisk form, när uppgifter skall gallras samt vilka rättigheter enskilda har. I vissa fall bör sådana bestämmelser vara ovillkorliga, medan regeringen i andra fall bör kunna medge undantag. Regeringen bör dessutom kunna meddela vissa kompletterande bestämmelser. Härigenom underlättas sådana anpassningar av regleringen som nödvändiggörs till följd av t.ex. den tekniska utvecklingen eller en ändrad inriktning av verksamheten. Lagförslagen i denna promemoria innehåller därför grundläggande och allmängiltiga bestämmelser om under vilka förutsättningar och för vilka ändamål Försvarsmakten och Försvarets radioanstalt i de aktuella verksamheterna över huvud taget får behandla personuppgifter om enskilda. Författningsförslagen innehåller även grundläggande bestämmelser om bl.a. förutsättningarna för att behandla känsliga personuppgifter. Sådana

bestämmelser får anses uppfylla kravet på en särskild lagreglering av registerföringen och databashantering. Det förhållandet påverkas inte av att de olika register och databaser som används i verksamheterna inte direkt omnämns i lagarna och att lagarna, i fråga om detaljer, överlåter regleringen åt regeringen. Med hänsyn till den tekniska och organisatoriska utvecklingen ändras ofta detaljerna i fråga om de olika register och databaser som finns, varför det är mindre ändamålsenligt att i lag befästa en viss register- eller databasstruktur. I den utsträckning föreskrifter om de register och databaser som används gemensamt i verksamheten är nödvändiga bör de därför lämnas i förordning.

7.2 Lagarnas förhållande till personuppgiftslagen

Förslag: Lagarna skall vara heltäckande och således innehålla alla de bestämmelser som skall vara tillämpliga för behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst samt Försvarets radioanstalts underrättelse- och utvecklingsverksamhet. Lagarna skall följaktligen återge de bestämmelser i personuppgiftslagen (1998:204) som skall tillämpas. En bestämmelse om förhållandet till personuppgiftslagen skall finnas i lagarna.

Utredningens förslag innebär att lagarna skall gälla i stället för personuppgiftslagen och att bestämmelser i personuppgiftslagen skall tillämpas endast när det anges särskilt.

Remissinstanserna: Flertalet remissinstanser tillstyrker förslaget eller har inga invändningar mot förslaget. *Rikspolisstyrelsen*, *Säkerhetspolisen* och *Kustbevakningen* förordar en lösning där lagarna är heltäckande och upprepar tillämpliga bestämmelser i personuppgiftslagen. *Säkerhetspolisen* anger att erfarenheten från tillämpningen av polisdatlagen (1988:622) är att det är opraktiskt att behöva arbeta med två olika lagar. *Kustbevakningen* anför att bestämmelserna i en heltäckande lag blir enkla och tydliga både för tillämpande myndigheter och för enskilda som

vill sätta sig in i regelsystemet, vilket är viktigt ur ett medborgarperspektiv.

Skäl för förslaget: Dataskyddsdirektivet genomförs genom personuppgiftslagen. Direktivet är inte tillämpligt på sådan behandling av personuppgifter som faller utanför gemenskapsrätten, d.v.s. behandling av personuppgifter inom verksamheter som rör t.ex. allmän säkerhet, försvar eller statens säkerhet. Personuppgiftslagen är emellertid generellt tillämplig på behandling av personuppgifter och omfattar således även behandling av personuppgifter inom verksamheter som faller utanför gemenskapsrätten. Om avvikande bestämmelser finns i andra författningar gäller dock dessa framför personuppgiftslagen. Personuppgiftslagen gäller således i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst samt i Försvarets radioanstalts underrättelseverksamhet, om det inte finns avvikande bestämmelser i lag eller förordning. Som anförts i avsnitt 7.1 är dessa verksamheter av sådan omfattning och karaktär att det med hänsyn till såväl effektivitets- som integritetsskäl är nödvändigt med avvikande bestämmelser från personuppgiftslagen. Det finns dock behov av vissa av bestämmelserna i personuppgiftslagen. Fråga uppstår då hur man skall hantera dessa bestämmelser. Olika modeller för detta har förekommit i tidigare lagstiftningsärenden.

Utöver personuppgiftslagen

En lagstiftningsmodell är att i en särskild författning inte alls nämna personuppgiftslagen eller ange att den särskilda författningen gäller utöver personuppgiftslagen. Detta innebär att personuppgiftslagens bestämmelser är tillämpliga när reglering saknas i den särskilda författningen. Modellen används idag i samtliga särskilda registerförfattningar förutom de fem lagar om behandling av personuppgifter inom skatt, tull och exekution som avses i prop. 2000/2001:33.

Istället för personuppgiftslagen

En annan modell är att i den särskilda författningen ange att den gäller istället för personuppgiftslagen och uttryckligen i författningen hänvisa till de lagrum i personuppgiftslagen som skall vara tillämpliga. De exempel på denna modell som finns är de fem lagarna beträffande behandling av personuppgifter inom skatt, tull och exekution. JO ansåg under remissförfarandet att den aktuella lagstiftningsmodellen kan innebära problem genom att det i vissa fall kan vara tveksamt hur en framtida ändring i personuppgiftslagen skall påverka speciallagen (prop. 2000/01:33 s. 87 f). Även Lagrådet hade synpunkter på den valda lagstiftningstekniken. Lagrådet ansåg att denna teknik var otillfredsställande och även riskfylld, med hänsyn såväl till svårigheterna att överblicka om dataskyddsdirektivet blir till fullo genomfört i registerlagstiftningen som till möjligheten att vid kommande lagändringar hänvisningarna till personuppgiftslagen blir felaktiga eller ofullständiga (nämnda prop. s. 345 f). Lagrådet krävde dock ingen ändring av den föreslagna lagstiftningstekniken. Regeringen motiverade valet av denna lagstiftningsteknik bl.a. med att den leder till att lagstiftningen blir överskådlig och tydlig (nämnda prop. s. 88). Regeringen konstaterade att lagstiftningsmodellen medför att en hel del av det merarbete det innebär för tillämparen att gå igenom den särskilda författningen och personuppgiftslagen parallellt och jämföra olika bestämmelser undanröjs. Vidare anförde regeringen att denna lagstiftningsteknik medför överskådlighet för den enskilde som därigenom lättare kan utnyttja de rättigheter som tillerkänns honom eller henne. Regeringen ansåg att, även om den föreslagna ordningen skiljde sig från den som dittills hade tillämpats, det mot bakgrund av den fördel det innebar borde anges i varje i propositionen aktuell lag vilka bestämmelser i personuppgiftslagen som är tillämpliga. Skatteutskottet tillstyrkte propositionen och gjorde inga uttalanden om lagstiftningstekniken som avvek från vad som anförts i propositionen (bet. 2000/01:SkU20). Riksdagen delade utskottets bedömning (rskr. 2000/01:176).

Förutom Underrättelsedatautredningen har såväl Domstolsdatautredningen som Tullbrottsdatautredningen i sina respektive betänkanden (SOU 2001:100 och SOU 2002:113) lämnat lagförslag som utgår från denna lagstiftningsteknik. I prop. 2004/05:164 Tullverkets brottsbekämpning – Effektivare uppgiftsbehandling föreslås en lag om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet som bygger på denna modell. Lagrådet hade inte några synpunkter på den valda lagstiftningstekniken.

Heltäckande lagteknisk lösning

En tredje lagstiftningsmodell är att i specialförfattningen samla alla de bestämmelser som skall vara tillämpliga för behandlingen av personuppgifter och således göra författningen heltäckande. De bestämmelser i personuppgiftslagen som skall vara tillämpliga upprepas följaktligen i specialförfattningen. En sådan modell har tidigare varit föremål för diskussion i några lagstiftningsärenden.

Av förarbetena till polisdatalagen framgår att flera remissinstanser hade synpunkter på den särskilda utredarens förslag att den nya lagen skulle gälla utöver personuppgiftslagen (prop. 1997/98:97 s. 97 f.). De förordade i stället att den nya lagen blev heltäckande. Regeringen ansåg att det skulle vara möjligt att upprepa personuppgiftslagens bestämmelser i den nya lagen, men att ett sådant system skulle bli väldigt tungrovt. Regeringen ansåg att man borde undvika en dubbelreglering och lämnade i propositionen ett lagförslag som innebar att polisdatalagen skulle gälla utöver personuppgiftslagen.

Polisdatautredningen har därefter vid sin översyn av polisdatalagen lämnat ett lagförslag som är heltäckande (SOU 2001:92). Av betänkandet framgår att det inom polisen framförts kritik mot konstruktionen med polisdatalagen som komplement till personuppgiftslagen och att det ansetts opraktiskt att arbeta med två olika lagar. Det är svårt för tillämparen att klart och tydligt se vilka bestämmelser i personuppgiftslagen som är tillämpliga och i vilken omfattning det i lagarna finns bestämmelser som kanske

endast delvis avviker från personuppgiftslagen. JO tillstyrkte i samband med remiss av betänkandet utredningens val av lagstiftningsteknik och anförde att den gör regelsystemet betydligt mera lättöverskådligt och lättillgängligt (se remissammanställning i Justitiedepartementets ärende dnr Ju2001/8624/PÅ). Rikspolisstyrelsen, som också tillstyrkte lagstiftningsmodellen, anförde att den nuvarande lagstiftningen skapar betydande problem för den enskilde lagtillämparen och angav som exempel att polismannen på fältet har att tillämpa såväl personuppgiftslagen och personuppgiftsförordningen som polisdatalagen och polisdataförordningen (1999:81). Polisdatautredningens förslag är föremål för beredning inom Regeringskansliet.

Statistikregelgruppen föreslog i sin promemoria Statistikens regler (Ds 1999:75 s. 106 f) att regleringen av behandling av personuppgifter för officiell statistik skulle arbetas in i en ny statistiklagstiftning som skulle ersätta den gällande särskilda registerlagstiftningen och personuppgiftslagens bestämmelser. Flertalet remissinstanser tillstyrkte statistikregelgruppens förslag eller hade inget att invända (se prop. 2000/01:27 s. 43 f). Några remissinstanser ställde sig emellertid tveksamma till den föreslagna modellen och menade att utredningen inte hade lyckats undvika de problem med oklarheter och tolkningssvårigheter som skulle motivera exklusiv tillämplighet för statistiklagens del. Regeringen konstaterade i nämnda proposition att det av remissutfallet framgick att det kunde uppkomma vissa oklara situationer om utredningens förslag skulle genomföras. Regeringen uttalade att det, som utredningen tänkt, naturligtvis hade varit önskvärt att kunna samla de regler som skall tillämpas för officiell statistik i en lag och en förordning. De redovisade tveksamheterna från remissinstanserna visade dock på svagheter i konstruktionen, varför regeringen ansåg att den av utredningen eftersträfvade regelförenklingen i detta avseende fick träda tillbaka för behovet av klarhet. Regeringen föreslog att en fortsatt särskild författningsreglering skulle gälla för behandling av personuppgifter för officiell statistik och att personuppgiftslagen skulle tillämpas i de fall

den särskilda författningen inte innehöll avvikande bestämmelser.

Överväganden och förslag

Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst och Försvarets radioanstalts underrättelseverksamhet utgör grundläggande och viktiga samhällsfunktioner för Sveriges oberoende och yttre säkerhet. Med hänsyn till verksamheternas speciella art finns det inte anledning att ställa krav på att de aktuella lagförslagen, såvitt gäller förhållandet till personuppgiftslagen, skall vara enhetliga med andra särskilda författningar om behandling av personuppgifter på t.ex. det brottsbekämpande området.

I verksamheterna behandlas en stor mängd personuppgifter och det är nödvändigt för myndigheterna att behandla även känsliga sådana uppgifter. Genom att samla alla tillämpliga bestämmelser om behandling av personuppgifter i en lag för Försvarmakten och en för Försvarets radioanstalt och i därtill hörande förordningar blir det överskådligt och tydligt för myndigheterna vad som gäller, vilket underlättar tillämpningen.

Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst och Försvarets radioanstalts underrättelseverksamhet är omgärdade av sekretessbestämmelser som försvårar möjligheten till den insyn som annars är möjlig i offentlig verksamhet. Det är därför särskilt viktigt att lagstiftningen utformas på ett sätt som underlättar för den enskilde att få klart för sig under vilka förutsättningar Försvarmakten och Försvarets radioanstalt kan komma att behandla personuppgifter som rör honom eller henne, samt under vilka förutsättningar den enskilde kan utnyttja de rättigheter som han eller hon har. En heltäckande lagstiftningslösning kan i detta perspektiv vara till fördel också för den enskilde.

Dataskyddsdirektivet är inte tillämpligt på sådan behandling av personuppgifter som skall regleras i de aktuella författningarna. Det finns således inte något behov av att kunna överblicka

om direktivet blivit korrekt genomfört på det aktuella området. Med en heltäckande lagstiftningsmodell undviks problemet med att hänvisningarna till personuppgiftslagen vid kommande lagändringar riskerar att bli felaktiga. Därmed undviks också den kritik som JO och Lagrådet framfört i det tidigare lagstiftningsärendet (jfr prop. 2000/01:33 s. 87 f och 345 f). Självfallet måste dock lagstiftningsarbete som innebär ändringar i personuppgiftslagen följas noggrant och ändringar i de nu aktuella lagarna göras i den mån det behövs. En förändrad syn på integritetsskyddet i allmänhet bör givetvis kunna få genomslag även på de nu aktuella områdena.

Sammantaget överväger i detta fall fördelarna med en heltäckande lagstiftningsteknik. De föreslagna lagarna om behandling av personuppgifter inom dels Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst, dels Försvarets radioanstalts underrättelseverksamhet bör därför innehålla alla de bestämmelser som skall gälla för behandlingen av personuppgifter på detta område.

För att det inte skall råda någon tvekan om att lagarna ersätter personuppgiftslagen skall detta förhållande framgå av en inledande bestämmelse i respektive lag.

7.3 Lagarnas allmänna tillämpningsområde

Förslag: De nya lagarna skall gälla vid behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst respektive i Försvarets radioanstalts underrättelse- och utvecklingsverksamhet, 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 som är tillgänglig för sökning eller sammanställning enligt särskilda kriterier.

Utredningens förslag överensstämmer i princip med promemorians. Utredningen föreslår att vissa bestämmelser i lagförsla-

gen även skall vara tillämpliga vid behandling av uppgifter om juridiska personer.

Remissinstanserna tillstyrker eller har inget att invända. *Hovrätten för Övre Norrland* anser dock att det bör övervägas om författningsregleringen kan ske gemensamt i en för Försvarsmakten och Försvarets radioanstalt tillämplig lag i stället för två särskilda lagar. Huvuddelen av bestämmelserna är enligt hovrätten identiska och avses ha samma innebörd och tillämpningsområde. Hovrätten anser därför att avvikelser i ordvalet bestämmelserna emellan bör förekomma endast när det är sakligt motiverat.

Skäl för förslaget: Som framgått av avsnitt 7.1 skall behandlingen av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst samt Försvarets radioanstalts underrättelse- och utvecklingsverksamhet regleras i lag. Vad försvarsunderrättelseverksamhet och säkerhetstjänst samt Försvarets radioanstalts underrättelse- och utvecklingsverksamhet inbegriper för verksamhet och behandling av personuppgifter har beskrivits i avsnitten 3 och 4. Begreppen försvarsunderrättelseverksamhet och militär säkerhetstjänst definieras inte särskilt i den föreslagna författningstexten. Inte heller beskrivs i författningstexten vad som innefattas i Försvarets radioanstalts underrättelse- och utvecklingsverksamhet. När det gäller att avgöra om en behandling omfattas av någon av de aktuella verksamheterna får ledning hämtas bl.a. från de författningar som reglerar dessa verksamheter. Bestämmelser om försvarsunderrättelseverksamhet finns i lagen (2000:130) om försvarsunderrättelseverksamhet och den därtill hörande förordningen. Grundläggande författningar vad gäller militär säkerhetstjänst är säkerhetskyddslagen (1996:627) och säkerhetskyddsförordningen (1996:633). Av förordningen (1994:714) med instruktion för Försvarets radioanstalt framgår att Försvarets radioanstalt har till uppgift att bedriva signalspaning och utvecklingsverksamhet.

I en inom Regeringskansliet upprättad departementspromemoria (Ds 2005:30) lämnas förslag till vissa ändringar i lagen om (2000:130) försvarsunderrättelseverksamheten. Därutöver läm-

nas i promemorian förslag till en lag om signalspaning och därtill hörande förordning som innebär att Försvarets radioanstalt får, för vissa i lagen angivna ändamål, inhämta signaler i elektronisk form. Förslagen har redovisats närmare i avsnitt 6. I denna promemoria har ändamålen för vilka behandling av personuppgifter får ske anpassats till de förslag som lämnas i nämnda promemoria.

Författningsregleringen skall inte omfatta behandling av personuppgifter i samband med de interna och administrativa åtgärder som kan förekomma i Försvarets radioanstalts verksamheter. För sådan behandling av personuppgifter gäller personuppgiftslagen (1998:204). Behandling av uppgifter om personalen kan dock komma att omfattas av lagarnas bestämmelser, om behandlingen sker för något av de ändamål som anges i lagarna. Sådan behandling kan förekomma i framför allt den militära säkerhetstjänsten.

De verksamheter som Försvarets radioanstalt bedriver och som omfattas av denna promemoria är inte identiska och de har endast till viss del samma syfte. Regleringen av Försvarets radioanstalts respektive Försvarets radioanstalts behandling av personuppgifter föranleder därför i flera avseenden olika rättsliga lösningar. Behandlingen av personuppgifter bör således inte, som föreslås av *Hovrätten för Övre Norrland*, regleras i en för Försvarets radioanstalt gemensam lag. Försvarets radioanstalts respektive Försvarets radioanstalts behandling av personuppgifter skall i stället regleras var för sig i två särskilda lagar.

Lagarna skall omfatta sådan behandling som avses i 5 § personuppgiftslagen. Detta innebär att lagarna skall omfatta helt eller delvis automatiserad behandling av personuppgifter och behandling av personuppgifter som ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier. Manuell behandling i t.ex. register omfattas alltså av lagstiftningen om uppgifterna är tillgängliga för sökning eller sammanställning enligt mer än ett kriterium.

Personuppgiftslagen gäller endast vid behandling av personuppgifter, dvs. all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet, 3 § personuppgiftslagen. Det innebär att behandling av uppgifter om juridiska personer inte omfattas av lagen. Försvarmakten och Försvarets radioanstalt behandlar i de aktuella verksamheterna uppgifter som rör andra än levande fysiska personer, t.ex. företag och organisationer. Som utredningen konstaterat har juridiska personer av naturliga skäl inte samma behov av integritetsskydd som levande fysiska personer. Det saknas därför anledning att gå längre än personuppgiftslagen och låta de föreslagna lagarna omfatta även behandlingen av juridiska personer. Lagförslagen skall således endast omfatta behandling av uppgifter om fysiska levande personer.

7.4 Syftet med lagarna

Förslag: Syftet med lagarna är att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst och i Försvarets radioanstalts underrättelse- och utvecklingsverksamhet. Lagarna bör innehålla en bestämmelse med detta innehåll.

Utredningen lämnar inget motsvarande förslag till bestämmelse.

Remissinstanserna: -

Skäl för förslaget: Av 2 kap. 3 § andra stycket regeringsformen framgår att varje medborgare skall, i den utsträckning som närmare anges i lag, skyddas mot att hans eller hennes personliga integritet kränks genom att uppgifter om honom eller henne registreras med hjälp av automatisk databehandling. Personuppgiftslagen (1998:204) är en sådan lag som närmare anger vilket skydd enskilda skall ha i detta avseende. Av 1 § personuppgiftslagen framgår att syftet med lagen är att skydda människor mot

att deras personliga integritet kränks genom behandling av personuppgifter.

Syftet med lagförslagen i denna promemoria är detsamma som syftet med personuppgiftslagen. En inledande bestämmelse om syftet bör tas in i de föreslagna lagarna.

7.5 Författningsstruktur

Förslag: De nya lagarna skall så långt det är möjligt och lämpligt följa strukturen i personuppgiftslagen samt vara likartade.

Utredningens förslag innebär att de nya lagarna skall ha samma inbördes systematik.

Remissinstanserna tillstyrker förslaget eller har ingen erinran.

Skäl för förslaget: De nya lagarna som föreslås skall vara heltäckande och upprepa de bestämmelser i personuppgiftslagen (1998:204) som skall vara tillämpliga (se avsnitt 7.2). Lagstiftningsarbete som innebär ändringar i personuppgiftslagen kan komma att medföra ändringar i de nu föreslagna lagarna. Det är därför en fördel om båda lagarna så långt det är möjligt och lämpligt följer strukturen i personuppgiftslagen samt är likartade.

De föreslagna lagarna är uppdelade i sex kapitel. Det första kapitlet innehåller allmänna bestämmelser om bl.a. tillämpningsområde, definitioner, personuppgiftsansvar och när behandling av personuppgifter är tillåten. Bestämmelserna skall tillämpas generellt på all behandling av personuppgifter. Bestämmelser om information till den enskilde, rättelse och skadestånd finns i det andra kapitlet. I det tredje kapitlet återfinns bestämmelser om säkerheten vid behandling. Det fjärde och femte kapitlet innehåller bestämmelser om anmälan till tillsynsmyndighet och tillsynsmyndighetens befogenheter. I det sjätte kapitlet återfinns övriga bestämmelser, såsom t.ex. bestämmelser om gallring och överklagande.

8 Bestämmelser om behandling av personuppgifter

8.1 Förhållandet till offentlighetsprincipen

Förslag: Bestämmelserna i lagarna skall inte tillämpas i den utsträckning det inskränker Försvarmaktens och Försvarets radioanstalts skyldighet enligt 2 kap. tryckfrihetsförordningen att lämna ut uppgifter.

Utredningen föreslår att bestämmelsen i 8 § personuppgiftslagen om förhållandet till offentlighetsprincipen i dess helhet skall gälla vid Försvarmaktens och Försvarets radioanstalts behandling av personuppgifter.

Remissinstanserna tillstyrker eller har inte något att erinra.

Skäl för förslaget: De grundläggande bestämmelserna om offentlighetsprincipen finns i 2 kap. tryckfrihetsförordningen (TF). I 2 kap. 1 § TF anges att varje svensk medborgare har rätt att ta del av allmänna handlingar. Denna rätt får enligt 2 kap. 2 § TF begränsas endast om det behövs med hänsyn till bl.a. rikets säkerhet eller dess förhållande till annan stat eller mellanfolklig organisation. Begränsningar i rätten att ta del av allmänna handlingar skall noga anges i en särskild lag eller annan lag som den särskilda lagen hänvisar till. Den särskilda lag som åsyftas är sekretesslagen (1980:100). Offentlighetsprincipen innebär således att myndigheterna är skyldiga att – i den utsträckning sekretess inte hindrar det – lämna ut allmänna handlingar till den som begär det.

Regeringen ansåg i samband med personuppgiftslagens (1998:204) tillkomst att det i klagörande syfte borde tas in en

bestämmelse i lagen som uttryckligen anger att bestämmelserna om offentlighetsprincipen i 2 kap. tryckfrihetsförordningen tar över bestämmelserna i lagen (prop. 1997/98:44 s. 46). I 8 § första stycket personuppgiftslagen finns således en bestämmelse som innehåller en upplysning om att lagen inte tillämpas om det skulle strida mot en myndighets skyldigheter enligt 2 kap. TF. Samma skäl gör sig gällande här och de i promemorian föreslagna lagarna skall därför innehålla en motsvarande upplysning.

I 8 § andra stycket första meningen personuppgiftslagen anges att bestämmelserna i lagen inte hindrar att en myndighet arkiverar och bevarar allmänna handlingar eller att arkivmaterial tas om hand av en arkivmyndighet. I avsnitt 8.20 behandlas frågan om en motsvarande bestämmelse skall återfinnas i de lagförslag som läggs fram här.

Av 8 § andra stycket andra meningen och 9 § fjärde stycket personuppgiftslagen följer att en myndighet får använda personuppgifter i allmänna handlingar som behandlas för historiska, statistiska eller vetenskapliga ändamål för att vidta åtgärder i fråga om den registrerade, utan att den registrerade har lämnat sitt samtycke eller att synnerliga skäl med hänsyn till den registrerades vitala intressen föreligger. Frågan om en motsvarande bestämmelse skall återfinnas i de lagförslag som lämnas här behandlas i avsnitt 8.4.

8.2 Definitioner

Förslag: Lagarna skall innehålla definitioner av begreppen behandling av personuppgifter, blockering av personuppgifter, mottagare, personuppgifter, personuppgiftsbiträde, personuppgiftsombud, den registrerade och tredje man. Definitionerna skall överensstämma med de som används i personuppgiftslagen (1998:204).

Utredningen föreslår att bestämmelsen i 3 § personuppgiftslagen som innehåller definitioner av olika begrepp skall gälla vid

Försvarsmaktens och Försvarets radioanstalts behandling av personuppgifter.

Remissinstanserna tillstyrker eller har inte något att erinra.

Skäl för förslaget: I de lagar som föreslås i denna promemoria används begreppen behandling av personuppgifter, blockering av personuppgifter, mottagare, personuppgifter, personuppgiftsansvarig, personuppgiftsbiträde, personuppgiftsombud, den registrerade, tillsynsmyndigheten och tredje man. Begreppen har hämtats från 3 § personuppgiftslagen, där centrala begrepp vid behandling av personuppgifter definieras. Begreppen har där följande betydelse.

- Med *behandling av personuppgifter* avses varje åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter, vare sig det sker på automatisk väg eller inte. Som exempel på behandling anges insamling, registrering, organisering, lagring, bearbetning eller ändring, återvinning, inhämtande, användning, utlämnande genom översändande, spridning eller annat tillhandahållande av uppgifter, sammanställning eller samkörning, blockering, utplåning eller förstöring.

- Med *blockering av personuppgifter* menas en åtgärd som vidtas för att personuppgifterna skall vara förknippade med information om att de är spärrade och om anledningen till spärren samt för att personuppgifterna inte skall lämnas ut till tredje man annat än med stöd av 2 kap. tryckfrihetsförordningen.

- *Mottagare* är den till vilken personuppgifter lämnas ut. När personuppgifter lämnas ut till en myndighet som skall utföra tillsyn, kontroll eller revision anses dock inte myndigheten som mottagare.

- Med *personuppgifter* menas all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet.

- *Personuppgiftsansvarig* är den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter.

- *Personuppgiftsbiträde* är den som behandlar personuppgifter för den personuppgiftsansvariges räkning.

- *Personuppgiftsombud* är den fysiska person som, efter förordnande av den personuppgiftsansvarige, självständigt skall se till att personuppgifter behandlas på ett korrekt och lagligt sätt.
- *Den registrerade* är den som en personuppgift avser.
- *Tillsynsmyndigheten* är den myndighet som regeringen utser för att utöva tillsyn.
- Med *tredje man* avses någon annan än den registrerade, den personuppgiftsansvarige, personuppgiftsombudet, personuppgiftsbiträdet och sådana personer som under den personuppgiftsansvariges eller personuppgiftsbitrådets direkta ansvar har befogenhet att behandla personuppgifter.

Med hänsyn till att begreppen i lagförslagen hämtats från 3 § personuppgiftslagen och att vissa av personuppgiftslagens bestämmelser återges i förslagen är det viktigt att terminologin överensstämmer. Om begreppen har samma innebörd i de olika lagarna undviks missförstånd. Definitioner av centrala begrepp som används i lagförslagen skall därför överensstämma med de i personuppgiftslagen.

I personuppgiftslagen definieras också vissa begrepp som inte återfinns i de i denna promemoria föreslagna lagarna. Vem som är personuppgiftsansvarig respektive tillsynsmyndighet framgår av 1 kap 5 § och 5 kap. 1 § i de båda lagförslagen. Det saknas därför anledning att definiera dessa begrepp.

Begreppet samtycke används inte i de nya lagarna. Det följer av de i promemorian aktuella verksamheternas natur att behandling av personuppgifter inte kan föregås av samtycke. Om en behandling i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst eller i Försvarets radioanstalts underrättelseverksamhet inte är motiverad med hänsyn till dess ändamål får den därför inte förekomma.

Begreppet tredje land är relevant för att ange länder som inte omfattas av dataskyddsdirektivet. Eftersom direktivet inte är tillämpligt på den verksamhet som regleras i de föreslagna lagarna finns det inte anledning att här använda begreppet.

8.3 Personuppgiftsansvar

Förslag: Försvarmakten respektive Försvarets radioanstalt skall vara personuppgiftsansvarig för den behandling som myndigheten utför. I personuppgiftsansvaret ingår att bestämma medlen för och, inom ramen för i lagarna angivna ändamål, de närmare ändamålen med behandlingen av personuppgifterna.

Utredningens förslag överensstämmer i princip med promemorians förslag. Utredningen föreslår att det särskilt skall markeras att personuppgiftsansvaret gäller också vid underlåtenhet att utföra behandling när sådan skall utföras. Utredningen föreslår därutöver att Försvarmakten och Försvarets radioanstalt även skall ha ansvar för att uppgifter om juridiska personer behandlas i enlighet med de grundläggande bestämmelserna i lagstiftningen.

Remissinstanserna tillstyrker eller har inget att invända mot utredningens förslag.

Skäl för förslaget: Med personuppgiftsansvarig avses den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandling av personuppgifter (se avsnitt 8.2). När det gäller behandling av personuppgifter i verksamheter som omfattas av en särskild reglering är dock ändamålen i regel angivna i den aktuella författningen. Det finns därför ett behov av att i den särskilda författningen genom en uttrycklig bestämmelse klargöra personuppgiftsansvaret för de behandlingar av personuppgifter som förekommer i en särskild bestämmelse. Så har t.ex. skett i 4 § lagen (2001:85) om behandling av personuppgifter i Tullverkets brottsbekämpande verksamhet och 6 § lagen (2003:763) om behandling av personuppgifter inom socialförsäkringens administration. Motsvarande bestämmelse föreslås också i förslaget till ny lag om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet (prop. 2004/05:164). Så bör ske även i de lagförslag som läggs fram här.

Även om det i lagarna anges för vilka ändamål behandling av personuppgifter får ske, bör det i bestämmelsen också erinras om att den personuppgiftsansvariga myndigheten inom denna ram

bestämmer de närmare ändamålen med behandlingen och medlen för denna.

Försvarmakten respektive Försvarets radioanstalt skall vara personuppgiftsansvariga för den behandling av personuppgifter som utförs inom respektive myndighets verksamhet. Personuppgiftsansvaret innebär bl.a. att Försvarmakten och Försvarets radioanstalt har ansvaret för att uppgifter som behandlas i t.ex. ett datorsystem är korrekta och att de inte behandlas på ett sätt som strider mot lagstiftningen eller de föreskrifter som meddelats med stöd av denna. Försvarmakten och Försvarets radioanstalt har givetvis ett ansvar inte endast för att utförd behandling är korrekt utan även för att behandling faktiskt utförs när den skall utföras (såsom t.ex. utlämnande av registerutdrag). Det finns inte anledning att, såsom utredningen föreslagit, särskilt markera att ansvaret gäller också en sådan underlåtenhet. En sådan markering saknas i de flesta andra särskilda författningar om behandling av personuppgifter.

Personuppgiftsansvaret enligt personuppgiftslagen täcker endast behandling av uppgifter om levande fysiska personer. De nu föreslagna lagarna skall såvitt gäller personuppgiftsansvaret inte gå längre än personuppgiftslagen (jfr. avsnitt 7.3). Försvarmaktens och Försvarets radioanstalts ansvar skall således inte omfatta behandling av uppgifter om avlidna personer eller, som utredningen föreslagit, om juridiska personer. Naturligtvis bör felaktiga uppgifter om dessa ändå rättas om felaktigheterna kommer till Försvarmaktens eller Försvarets radioanstalts kännedom.

8.4 Grundläggande krav på behandling av personuppgifter

Förslag: Försvarmakten respektive Försvarets radioanstalt skall se till att

1. personuppgifter alltid behandlas på ett korrekt sätt och i enlighet med god sed,
2. personuppgifter samlas in bara för särskilda, uttryckligt angivna och berättigade ändamål,

3. personuppgifter inte behandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in,
4. de personuppgifter som behandlas är adekvata och relevanta i förhållande till ändamålen med behandlingen,
5. inte fler personuppgifter behandlas än som är nödvändigt med hänsyn till ändamålen med behandlingen,
6. de personuppgifter som behandlas är riktiga och, om det är nödvändigt, aktuella, och
7. alla rimliga åtgärder vidtas för att rätta, blockera eller utplåna sådana personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålen med behandlingen.

Utredningen föreslår att bestämmelsen i 9 § personuppgiftslagen (1998:204) om grundläggande krav på behandlingen av personuppgifter i dess helhet skall gälla vid Försvarmaktens och Försvarets radioanstalts behandling av personuppgifter.

Remissinstanserna tillstyrker eller har inte något att invända.

Skäl för förslaget: I 9 § personuppgiftslagen anges de grundläggande kraven på behandling av personuppgifter som den personuppgiftsansvarige alltid måste uppfylla vid sin behandling. Bestämmelsen har sitt ursprung i dataskyddsdirektivet.

Det är självfallet viktigt att de grundläggande krav som uppställs för behandling av personuppgifter i allmänhet gäller även för behandling av personuppgifter i de verksamheter som regleras här. En bestämmelse motsvarande den i 9 § personuppgiftslagen bör därför återfinnas i de lagförslag som lämnas i denna promemoria, dock med vissa inskränkningar. I det följande redovisas de överväganden som gjorts.

Behandling bara om det är lagligt

Personuppgifter får enligt 9 § första stycket i personuppgiftslagen bara behandlas om det är lagligt. När det är lagligt att behandla personuppgifter framgår av andra bestämmelser i personuppgiftslagen, såsom t.ex. 10 och 13–20 §§. Bestämmelsen i 9 § har sin bakgrund i dataskyddsdirektivet där en motsvarande be-

stämmelse finns. Det är osäkert om sistnämnda bestämmelse har någon självständig betydelse. Bestämmelsen har tagits med i personuppgiftslagen för säkerhets och fullständighetens skull (SOU 1997:39 s. 350).

Behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst samt Försvarets radioanstalts underrättelse- och utvecklingsverksamhet regleras uttömmande i de lagförslag som lämnas i denna promemoria och de förordningar som kommer att utarbetas och ansluta till respektive lag. Det följer av sakens natur att en behandling av personuppgifter måste ske i enlighet med bestämmelserna i dessa författningar för att den skall anses vara laglig. En bestämmelse motsvarande den i 9 § första stycket a personuppgiftslagen är därför överflödig. Skulle i undantagsfall någon vid myndigheten t.ex. inhämtat personuppgifter på ett sätt som är olagligt och straffbart kan för övrigt dessa personuppgifter inte anses ha behandlats på ett korrekt sätt (se nedan).

Behandling på ett korrekt sätt och i enlighet med god sed

Personuppgifter skall alltid behandlas på ett korrekt sätt och i enlighet med god sed, 9 § första stycket b personuppgiftslagen. Det är osäkert om också denna bestämmelse har någon självständig betydelse. Även den har tagits med i personuppgiftslagen för säkerhets och fullständighetens skull (SOU 1997:39 s. 350). Kravet på att personuppgifter skall behandlas i enlighet med god sed har inte någon motsvarighet i dataskyddsdirektivet utan är en svensk konstruktion. Vad som är god sed vid personuppgiftsbehandling får avgöras i rättstillämpningen mot bakgrund av bl.a. de mer preciserade föreskrifter som kan utfärdas med stöd av lagen och hur ansvarsfulla personuppgiftsansvariga som regel beter sig (prop. 1997/98:44 s. 143). En motsvarande bestämmelse bör återfinnas i lagförslagen.

Insamling för särskilda, uttryckligt angivna och berättigade ändamål

Personuppgifter skall enligt 9 § första stycket c personuppgiftslagen samlas in bara för särskilda, uttryckligt angivna och berättigade ändamål. Detta innebär att ändamålen med en behandling av personuppgifter måste bestämmas redan när uppgifterna samlas in. Det är den personuppgiftsansvarige som normalt sett ensam eller tillsammans med andra bestämmer ändamålen för behandling av personuppgifter. Det är, liksom vad gäller bestämmelserna om laglig och korrekt behandling, osäkert om bestämmelsen om berättigade ändamål har någon självständig betydelse. Även den har dock tagits med i personuppgiftslagen för säkerhets och fullständighets skull (SOU 1997:39 s. 350).

När det gäller behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst samt Försvarets radioanstalts underrättelse- och utvecklingsverksamhet är de övergripande ändamålen för behandling uttömmande angivna i de lagförslag som läggs fram här. Försvarsmakten respektive Försvarets radioanstalt har dock att inom ramen för vad lagen anger i varje enskilt fall bestämma de närmare särskilda ändamål för vilka personuppgifter behandlas. Det finns därför skäl att i lagförslagen ha med en bestämmelse motsvarande den i 9 § första stycket c personuppgiftslagen.

Behandling endast för ändamål som inte är oförenligt med det för vilket uppgifterna samlades in

Insamlade uppgifter får behandlas för andra ändamål än de för vilka uppgifterna samlades in bara om de nya ändamålen inte är oförenliga med de ursprungliga ändamålen, 9 § första stycket d personuppgiftslagen. Vad som är oförenligt med de ursprungliga ändamålen får bestämmas genom praxis. Bestämmelsen begränsar i praktiken möjligheterna till samkörning av register. Den innebär också att den personuppgiftsansvarige under hela behandlingstiden måste hålla reda på för vilka ändamål varje per-

sonuppgift har samlats in. En bestämmelse med motsvarande innehåll bör finnas i de föreslagna lagarna.

Vid tillämpning av de föreslagna lagarna kan fråga uppstå om i vilken utsträckning det är tillåtet att i t.ex. den militära säkerhetstjänsten behandla uppgifter som insamlats för de ändamål som i lagen anges för försvarsunderrättelseverksamheten och vice versa. Ur verksamhetssynpunkt föreligger i många fall ett behov av att kunna använda uppgifter på detta sätt. Verksamheterna har många beröringspunkter och bedrivs inom samma organisatoriska enheter. Det är inte sällan en uppgift har betydelse för såväl försvarsunderrättelseverksamheten som säkerhetstjänsten och det kan vara slumpen som avgör inom vilken verksamhet uppgiften insamlas. Efterhand som en personuppgift kompletteras med ytterligare information kan det också visa sig att den är mer relevant för den andra verksamheten, inom vilken den inte ursprungligen inhämtades. Eftersom behandling av personuppgifter för annat ändamål än det för vilket uppgifterna samlades in är otillåtet endast om det nya ändamålet är *oförenligt* med det ursprungliga finns utrymme för att behandla en personuppgift i båda verksamheterna eller att behandla en uppgift i en annan verksamhet än den i vilken uppgiften samlades in. Frågan måste emellertid bedömas från fall till fall. Genom den särskilda granskningsuppgift som anförtros Försvarets underrättelsenämnd (se vidare avsnitt 8.16) finns förutsättningar för att skapa enhetliga riktlinjer på detta område.

Bestämmelsen kan också aktualiseras i samband med utlämnande av uppgifter, se vidare avsnitt 8.21.

Personuppgifterna skall vara adekvata och relevanta

De behandlade uppgifterna skall vara adekvata och relevanta i förhållande till ändamålet med behandlingen, 9 § första stycket i personuppgiftslagen. Detta innebär bl.a. att ovidkommande uppgifter inte får behandlas. En motsvarande bestämmelse bör finnas i lagförslagen.

Inte behandling av fler personuppgifter än nödvändigt

Det är inte tillåtet att behandla fler personuppgifter än som är nödvändigt med hänsyn till ändamålet med behandlingen, 9 § första stycket f personuppgiftslagen. Det är i första hand den personuppgiftsansvarige som har att bedöma vilka och hur många uppgifter som det är nödvändigt att behandla för att uppfylla ändamålen med behandlingen. En bestämmelse med samma innehåll bör återfinnas i lagförslagen.

Personuppgifterna skall vara riktiga och aktuella

De behandlade uppgifterna skall vara riktiga och, om det är nödvändigt, aktuella, 9 § första stycket g personuppgiftslagen. Uppgifter som är felaktiga eller ofullständiga i förhållande till de ändamål för vilka uppgifterna behandlas accepteras inte och måste rättas, blockeras eller utplånas (se nedan angående 9 § första stycket h). Datalagskommittén underströk vikten av att de behandlade uppgifterna håller en hög kvalitet. Användningen av felaktiga, missvisande eller ofullständiga uppgifter kan förorsaka registrerade och andra stora skador och stor förtret i övrigt. Sådana olägenheter kunde, enligt Datalagskommittén, förebyggas genom en sund källkritik kombinerad med nödvändig noggrannhet och genom att det dokumenteras varifrån olika uppgifter har hämtats (SOU 1997:39 s. 351 f). En motsvarande bestämmelse bör återfinnas i lagförslagen.

Rimliga åtgärder skall vidtas för att korrigera personuppgifter

Den personuppgiftsansvarige måste självmant vidta alla rimliga åtgärder för att rätta, blockera eller utplåna sådana personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålet med behandlingen, 9 § första stycket h. Den personuppgiftsansvarige har här således en skyldighet att vara aktiv. Lagförslagen bör innehålla en bestämmelse med motsvarande innehåll.

Bevarande av personuppgifter

Personuppgifter får, enligt 9 § första stycket i personuppgiftslagen, inte bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen. Bestämmelsen behandlas i avsnitt 8.20.

Behandling för historiska, statistiska eller vetenskapliga ändamål

Lagring och annan behandling av personuppgifter för historiska, statistiska och vetenskapliga ändamål är särskild gynnad i personuppgiftslagen. Av 9 § andra och tredje styckena personuppgiftslagen framgår att personuppgifter kan användas för historiska, statistiska och vetenskapliga ändamål oavsett för vilka ändamål uppgifterna samlades in. Vidare framgår att personuppgifter får bevaras för historiska, statistiska eller vetenskapliga ändamål under längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen, dock inte under längre tid än vad som behövs för dessa ändamål.

Myndigheternas arkivering av allmänna handlingar som inte gallras (se avsnitt 8.20) får även utan uttrycklig bestämmelse därom anses förenlig med de ursprungligen bestämda ändamålen med behandlingen. Det saknas därför skäl att i lagarna föra in bestämmelser om arkivering.

Av 8 § andra stycket sista meningen och 9 § fjärde stycket personuppgiftslagen följer att myndigheter får använda personuppgifter i allmänna handlingar som behandlas för historiska, statistiska eller vetenskapliga ändamål för att vidta åtgärder i fråga om den registrerade, utan att samtycke har lämnats av den registrerade eller sådana synnerliga skäl med hänsyn till den registrerades vitala intressen föreligger. Varken Försvarsmakten eller Försvarets radioanstalt använder personuppgifter som behandlas för sådana ändamål för att vidta åtgärder beträffande den registrerade. Det saknas därför anledning att införa en bestämmelse motsvarande den i personuppgiftslagen i lagförslagen.

8.5 När behandling av personuppgifter är tillåten

Förslag:

Försvarmakten

Personuppgifter får behandlas i Försvarmaktens försvarsunderrättelseverksamhet om det är nödvändigt för att bedriva den verksamhet som anges i lagen (2000:130) om försvarsunderrättelseverksamhet.

Uppgifter om en person får endast behandlas om personen har anknytning till en preciserad inriktning för försvarsunderrättelseverksamheten och behandlingen är nödvändig för att fullfölja den inriktningen.

Vidare får personuppgifter behandlas i den militära säkerhetstjänstens verksamhet med att upptäcka, förebygga och avvärja säkerhetshotande verksamhet som riktas mot Försvarmakten och dess säkerhetsintressen, om det är nödvändigt för att

1. klarlägga verksamhet som innefattar hot mot rikets säkerhet, eller
2. vidta åtgärder som hindrar eller försvårar säkerhetshotande verksamhet.

Försvarets radioanstalt

Personuppgifter får behandlas i Försvarets radioanstalts försvarsunderrättelseverksamhet om det är nödvändigt för att bedriva den verksamhet som anges i lagen (2000:130) om försvarsunderrättelseverksamhet.

Uppgifter om en person får endast behandlas om personen har anknytning till en preciserad inriktning för försvarsunderrättelseverksamheten och behandlingen är nödvändig för att fullfölja den inriktningen.

Personuppgifter får vidare behandlas av myndigheten i sådan underrättelseverksamhet som inte omfattas av försvarsunderrättelseverksamhet, om det är nödvändigt för att, i enlighet med vad regeringen bestämmer

1. följa förändringen av signalmiljön i omvärlden, den tekniska utvecklingen och signalskyddet, samt

2. fortlöpande utveckla den teknik och metodik som behövs för att bedriva verksamheten.

Personuppgifter får därutöver behandlas av Försvarets radioanstalt om det är nödvändigt för att biträda andra myndigheter vid värdering, utveckling, anskaffning och drift av signalspaningssystem. Sådana personuppgifter får inte användas för något annat ändamål eller lämnas ut till annan.

Utredningens förslag överensstämmer i princip med promemorians. Utredningen har dock valt en annan lösning än att hänvisa till lagen (2000:130) om försvarsunderrättelseverksamhet. Utredningen föreslår vidare att bestämmelsen om behandling i Försvarets radioanstalts utvecklingsverksamhet också skall omfatta att utföra matematiska bedömningar av kryptosystem för totalförsvaret.

Remissinstanserna: De flesta remissinstanser tillstyrker eller har inget att invända mot de föreslagna ändamålen. *Justitiekanslern* anser att de ändamål för vilka behandling av personuppgifter får ske förefaller väl avgränsade och att skyddet för enskildas personliga integritet tycks ha beaktats så långt som det är möjligt med hänsyn till verksamhetens speciella art. *Försvarsmakten* framför att signalskyddet enligt regleringsbrevet för Försvarmakten är en säkerhetsskyddsangelägenhet och således inte en självständig del av den militära säkerhetstjänsten. I och med detta behöver, enligt Försvarmakten, inte denna funktion regleras separat utöver de bestämmelser som gäller för säkerhetsskyddet i övrigt i den föreslagna lagen. Försvarmakten anser att det är obehövt att i den föreslagna lagen ange de olika verksamhetsgrenarna inom den militära säkerhetstjänsten. *Försvarets radioanstalt* anser att personuppgifter som får behandlas om det behövs för myndighetens verksamhet med att utföra matematiska bedömningar av kryptosystem inte skall vara begränsade till bedömningar av kryptosystem för totalförsvaret.

Skäl för förslaget:

Personuppgiftslagen

I 10–12 §§ personuppgiftslagen (1998:204) finns bestämmelser om när det överhuvudtaget är tillåtet att behandla personuppgifter. Det krävs som huvudregel samtycke för att personuppgifter skall få behandlas, 10 §. Den registrerade har rätt att när som helst återkalla sitt samtycke, 12 §. Behandling av personuppgifter får dock ske utan samtycke under vissa förutsättningar som närmare anges i 10 §. Exempelvis får behandling av personuppgifter ske om den är nödvändig för att en arbetsuppgift av allmänt intresse skall kunna utföras. Behandling av personuppgifter får också ske om den är nödvändig för att ett ändamål som rör ett berättigat intresse hos den personuppgiftsansvarige skall kunna tillgodoses. Det förutsätter dock att detta intresse väger tyngre än den registrerades intresse av skydd mot kränkning av den personliga integriteten. Bestämmelsen i 10 § innehåller en uttömmande uppräkningslista av i vilka fall behandling av personuppgifter är tillåten. Om en behandling inte kan hänföras till något av de fall som anges där är behandlingen otillåten och får inte genomföras. Om behandlingen avser t.ex. känsliga personuppgifter måste behandlingen också vara tillåten enligt bestämmelserna om behandlingen av sådana uppgifter, 14–19 §§. Även de grundläggande kraven på behandling i 9 § måste vara uppfyllda.

Bestämmelsen i 10 § är allmänt hållen och av naturliga skäl inte anpassad till de verksamheter som Försvarmakten och Försvarets radioanstalt bedriver. Behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst respektive i Försvarets radioanstalts underrättelse- och utvecklingsverksamhet kan av naturliga skäl inte grunda sig på samtycke från den enskilde. Om en behandling av personuppgifter i dessa verksamheter inte är motiverad med hänsyn till ändamålen för verksamheterna får den överhuvudtaget inte förekomma. I de lagförslag som läggs fram här finnas således bestämmelser om tillåtna ändamål för personuppgiftsbehandling

som knyter an till Försvarsmaktens respektive Försvarets radioanstalts verksamheter. Bestämmelserna anger uttömmande i vilka fall personuppgifter får behandlas. Avser behandlingen känsliga personuppgifter eller personnummer eller samordningsnummer måste behandlingen dessutom vara tillåten enligt de särskilda bestämmelser i lagförslagen som reglerar behandling av sådana uppgifter. Även de grundläggande kraven på behandling av personuppgifter måste vara uppfyllda.

Ändamålsbestämmelserna måste vara tillräckligt tydliga och konkreta för att det skall kunna avgöras i vilken utsträckning myndigheternas personuppgiftsbehandling håller sig inom angivna ramar. Samtidigt är verksamheten av sådan art sådan att det inte ansetts möjligt att i lagform reglera den i detalj (prop. 1999/2000:24 s. 12), vilket måste beaktas vid utformningen av ändamålsbestämmelserna. Det är följaktligen oundvikligt att ändamålsbestämmelserna lämnar ett visst mått av utrymme för myndigheterna att bedöma om en behandling ryms inom det angivna ändamålet eller inte. Den särskilda granskning av verksamheten som redogörs för i avsnitt 8.16 säkerställer i tillräcklig utsträckning att denna bedömningsmån inte utnyttjas på ett sätt som medför risker för kränkning av enskildas personliga integritet.

Försvarsmaktens försvarsunderrättelseverksamhet

Som framgått av avsnitt 3 åligger det Försvarsmakten enligt lagen (2000:130) om försvarsunderrättelseverksamhet och den därtill hörande förordningen att bedriva försvarsunderrättelseverksamhet för att kartlägga yttre militära hot mot landet och till stöd för svensk utrikes-, försvars- och säkerhetspolitik. I verksamheten ingår att medverka i svenskt deltagande i internationellt säkerhetssamarbete och att, enligt vad regeringen närmare bestämmer, medverka med underrättelser för att stärka samhället vid svåra påfrestningar på samhället i fred. Regeringen bestämmer enligt lagen verksamhetens inriktning.

I den inom Regeringskansliet upprättade departementspromemorian Ds 2005:30 föreslås de ändringar i lagen om försvarsunderrättelseverksamhet som redovisats i avsnitt 6.1. Underrättelsetjänsterna skall i huvudsak delge strategiska underrättelser av relevans för utrikes-, säkerhets- och försvarspolitiken. I verksamheten skall ingå, enligt promemorians förslag, att kartlägga yttre hot mot landet och att, liksom redan idag, medverka i svenskt deltagande i internationellt säkerhetssamarbete. Verksamheten får endast avse utländska förhållanden. Att försvarsunderrättelsemyndigheterna kan medverka med underrättelser för att stärka samhället vid svåra påfrestningar på samhället i fred behöver, enligt promemorian, inte komma till särskilt uttryck i lagen eftersom detta omfattas av begreppet yttre hot mot landet. Försvarsunderrättelseverksamheten skall även fortsättningsvis bedrivas i enlighet med regeringens inriktning.

De uppgifter som idag behandlas i Försvarsmaktens försvarsunderrättelseverksamhet och som även fortsättningsvis kommer att behandlas där kan avse alla typer av uppgifter, såväl personuppgifter som andra uppgifter vilka inte alls kan hänföras till en viss person. De personuppgifter som behandlas är bl.a. uppgifter om personer som verkar inom andra staters försvars- eller underrättelseväsende, ledande politiska företrädare och andra opinionsbildare samt andra personer som förekommer i underrättelse rapporter eller kan komma att få ett underrättelsevärde (se avsnitt 3.3).

Försvarsunderrättelser utgörs av säkerhetspolitiska och militärstrategiska bedömningar, analyser av pågående och framtida konflikter samt biografiska underrättelser, som avser personlig information om militär personal och andra viktiga befattningshavare.

Ändamålet för Försvarsmaktens behandling av personuppgifter i försvarsunderrättelseverksamheten är att myndigheten skall kunna utföra de uppgifter som åligger myndigheten enligt lagen om försvarsunderrättelseverksamhet och den därtill hörande förordningen. De närmare riktlinjerna för verksamheten läggs fast av regeringen bl.a. genom det årliga inriktningsbeslutet. Det

är inte möjligt att här definiera gränserna för försvarsunderrättelseverksamheten på något annat sätt än enligt lagen om försvarsunderrättelseverksamhet. Det finns inte heller anledning att upprepa innehållet i denna lag. Här föreslås därför att personuppgifter skall få behandlas i Försvarsmaktens försvarsunderrättelseverksamhet om det är nödvändigt för att bedriva den verksamhet som anges i lagen om försvarsunderrättelseverksamhet. En sådan hänvisning innebär att ändamålet med personuppgiftsbehandlingen begränsas på samma sätt som försvarsunderrättelseverksamheten i stort, bl.a. med avseende på gränsdragningen mot polisiär verksamhet. Av förslagen i Ds 2005:30 framgår att försvarsunderrättelseverksamhet inte skall få innefatta åtgärder som ligger inom ramen för polisens och andra myndigheters brottsbekämpande och brottsförebyggande arbete enligt lagar och förordningar. Utan hinder av denna begränsning skall försvarsunderrättelseverksamhet dock, under förutsättning att den inte riktar sig mot fysisk person, få bedrivas för kartläggning av utländska förhållanden som innebär yttre hot mot landet.

Utöver bestämmelserna i lagen om försvarsunderrättelseverksamhet styrs verksamheten av regeringens inriktning, vilken ytterligare avgränsar de ändamål för vilka verksamheten får bedrivas. Försvarsmakten producerar dessutom interna styrdokument där en ytterligare precisering i förhållande till regeringens inriktning görs. Försvarsmakten bestämmer på detta sätt närmare ändamålen för verksamheten – och därmed ramen för behandlingen av personuppgifter – i enlighet med vad uppgiften som personuppgiftsansvarig ålägger myndigheten, se avsnitt 8.3.

Som framhållits ovan är det inte möjligt att i lagtext närmare precisera de ändamål för vilka personuppgifter får behandlas i försvarsunderrättelseverksamheten. Det innebär att kontrollfunktionen blir ett viktigt inslag för att säkerställa att behandlingen sker inom ramen för verksamhetens ändamål, så som de anges i de olika styrdokumenterna. Den myndighetsinterna inriktningen, med dess preciserade ändamålsangivelse, är därvid vid sidan av författningsregleringen och regeringens inriktning en väsentlig utgångspunkt för granskningen. Genom den föreslagna

hänvisningen till lagen om försvarsunderrättelseverksamhet framgår att såväl de direkt i lagen angivna ändamålen som de ändamål som återfinns i regeringens inriktning utgör avgränsningar för behandlingen av personuppgifter. Bestämmelsen bör mot bakgrund av ovanstående också kompletteras med begränsningen att uppgifter om en person endast får behandlas om personen har anknytning till en preciserad inriktning för försvarsunderrättelseverksamheten och behandlingen är nödvändig för att fullfölja den inriktningen. Med *preciserad inriktning* avses de interna inriktningar som Försvarsmakten fastställer för närmare avgränsning av verksamheten.

Militär säkerhetstjänst

Den militära säkerhetstjänsten har till uppgift att upptäcka, identifiera och möta säkerhetshot som riktas mot Försvarsmakten och dess säkerhetsintressen såväl inom som utom landet, se redogörelse i avsnitt 3. Säkerhetsskyddslagen (1996:627) och den därtill knutna förordningen innebär att Försvarsmakten dels måste ha det säkerhetsskydd som behövs med hänsyn till verksamhetens art, omfattning m.m., dels har att utöva tillsyn av säkerhetsskyddet hos vissa myndigheter.

Den militära säkerhetstjänsten omfattar säkerhetsunderrättelsetjänst och säkerhetsskyddstjänst. Säkerhetsunderrättelsetjänsten syftar till att klarlägga den säkerhetshotande verksamhetens omfattning m.m. och att utifrån säkerhetsunderrättelsebehov lämna underlag för beslut om bl.a. säkerhetsskyddsåtgärder. Säkerhetsskyddstjänstens uppgift är att vidta olika åtgärder för att förhindra eller försvåra säkerhetshotande verksamhet. Inom säkerhetsskyddstjänsten arbetar man bl.a. med att förebygga att hemliga uppgifter som rör rikets säkerhet obehörigen röjs, ändras eller förstörs. Säkerhetsskyddstjänsten syftar också till att skydda Försvarsmaktens personal, materiel och anläggningar. Signalskyddstjänsten är en säkerhetsskyddsangelägenhet och avser att minska verkan av signalspaning, falsk signalering och störsändning mot totalförsvarets telekommunikations- och informa-

tionssystem. Signalskyddstjänsten skall förhindra obehörig insyn i och påverkan av totalförsvarets telekommunikationer samt verka för att sekretessbelagda uppgifter och andra skyddsvärda uppgifter skyddas av kryptografiska funktioner i informationssystem. En viktig del av signalskyddstjänsten är kontroll av signalskydd (signalkontroll) i Försvarmaktens telekommunikations- och informationssystem. Genom signalkontroll klarläggs bl.a. riskerna för att obehöriga får åtkomst till data eller för att dessa stör eller manipulerar data. Vidare klarläggs genom signalkontroll att systemen används enligt gällande regler.

I den militära säkerhetstjänsten behandlas uppgifter om t.ex. personer vid andra staters underrättelseväsenden eller annan företrädare för främmande makt som bedöms kunna utgöra ett säkerhetshot och personer som deltagit eller på annat sätt har anknytning till säkerhetshotande verksamhet. Personuppgifter behandlas även i anledning av att någon varit föremål för säkerhetsprövning enligt säkerhetsskyddslagen om denne är anställd inom Försvarmakten eller har anknytning till säkerhetsskyddad upphandling. Vidare behandlas uppgifter om personer som av annan anledning är av betydelse för den militära säkerhetstjänsten och dess tillsynsområde.

Ändamålet med behandlingen av personuppgifter inom den militära säkerhetstjänsten är att tjänsten skall kunna fullgöra de uppgifter som följer av säkerhetsskyddslagen, den därtill hörande förordningen och förordningen (2000:555) med instruktion för Försvarmakten. Här föreslås därför att personuppgifter skall få behandlas i den militära säkerhetstjänstens verksamhet med att upptäcka, förebygga och avvärja säkerhetshotande verksamhet som riktas mot Försvarmakten och dess säkerhetsintressen, om det är nödvändigt för att klarlägga verksamhet som innefattar hot mot rikets säkerhet. Denna säkerhetsverksamhet kallas för säkerhetsunderrättelsetjänst. I samma syfte skall personuppgifter få behandlas, om det är nödvändigt för att vidta åtgärder som hindrar eller försvårar säkerhetshotande verksamhet. Det är här fråga om säkerhetsskyddstjänst. Även inom signalskyddstjän-

ten, som är en säkerhetsskyddsangelägenhet, kan arbete förekomma som avser att klarlägga säkerhetshotande verksamhet.

Som angetts av Försvarmakten är signalskyddstjänsten en säkerhetsskyddsangelägenhet och innefattar, liksom säkerhetsskyddstjänsten, åtgärder för att hindra eller försvåra säkerhetshotande verksamhet. Den behöver därför inte, såsom föreslagits av utredningen, regleras särskilt. Det saknas, som Försvarmakten anfört, behov av att i lagen ange de olika verksamhetsgrenarna inom den militära säkerhetstjänsten.

I avsnitt 8.6 lämnas förslag på en särskild bestämmelse om vilka personer som får registreras i den militära säkerhetstjänsten.

Försvarets radioanstalts underrättelse- och utvecklingsverksamhet

Försvarets radioanstalt har idag, liksom bland annat Försvarmakten, till uppgift att bedriva försvarsunderrättelseverksamhet (se ovan beträffande Försvarmakten och avsnitt 4).

Som framgått föreslås i departementspromemorian Ds 2005:30 vissa ändringar i lagen om försvarsunderrättelseverksamhet (se vidare avsnitt 6).

De uppgifter som Försvarets radioanstalt behandlar i försvarsunderrättelseverksamheten är information som i huvudsak är av strategisk betydelse för bedömningar av den allmänna utrikes- och försvarspolitiska utvecklingen samt internationella relationer. Även information om krishärdar och de internationella uppdrag i vilka svensk personal deltar behandlas. Därutöver delges viss information rörande bl.a. händelser i närheten av svenskt territorium. Rapporteringen av underrättelser kan t.ex. röra främmande stridskrafterns rörelser, övningar och prov av vapen samt kränkningar av svenskt territorium. I underrättelseverksamheten ingår också rapportering av biografiska underrättelser. De personuppgifter som behandlas är bl.a. uppgifter om personer som verkar inom andra staters försvars- och underrättelseväsenden, ledande politiska företrädare och andra opinionsbildare samt andra personer som förekommer i underrättelserapporter eller kan komma att få ett underrättelsevärde.

Ändamålet för Försvarets radioanstalts behandling av personuppgifter i försvarsunderrättelseverksamheten är att myndigheten skall kunna utföra de uppgifter som åligger den enligt lagen och förordningen om försvarsunderrättelseverksamhet. I denna promemoria föreslås således på motsvarande sätt som beträffande Försvarsmakten att personuppgifter skall få behandlas i Försvarets radioanstalts försvarsunderrättelseverksamhet om det är nödvändigt för att bedriva den verksamhet som anges i lagen om försvarsunderrättelseverksamhet.

På motsvarande sätt som när det gäller Försvarsmakten bör i den ändamålsbestämmelse som avser försvarsunderrättelseverksamhet också anges att uppgifter om en person endast får behandlas om personen har en klar anknytning till en preciserad inriktning för verksamheten och behandlingen är nödvändig för att fullfölja den inriktningen. Med *preciserad inriktning* avses, liksom i fråga om Försvarsmakten, de interna inriktningar som myndigheten fastställer för närmare avgränsning av verksamheten.

Försvarets radioanstalt bedriver även annan *underrättelseverksamhet* än försvarsunderrättelseverksamhet (se avsnitt 4.1). Försvarets radioanstalt bedriver t. ex. underrättelseverksamhet som syftar till att följa förändringen av signalmiljön i omvärlden, den tekniska utvecklingen och signalskyddet samt fortlöpande utveckla den teknik och metodik som behövs för att bedriva verksamheten, 2 § instruktionen. I promemorian Ds 2005:30 lämnas förslag till en lag om signalspaning som innebär att Försvarets radioanstalt skall få inhämta signaler i elektronisk form för dessa ändamål. I promemorian föreslås att regeringen skall bestämma inriktningen av denna verksamhet (se vidare avsnitt 6).

Här föreslås därför att Försvarets radioanstalt skall få behandla personuppgifter i sådan underrättelseverksamhet som inte omfattas av försvarsunderrättelseverksamhet, om det är nödvändigt för att, i enlighet med vad regeringen bestämmer, följa förändringen i signalmiljön i omvärlden, den tekniska utvecklingen och signalskyddet samt för att fortlöpande utveckla den teknik och metodik som behövs för att bedriva verksamheten.

Försvarets radioanstalt bedriver, utöver underrättelseverksamhet, viss *utvecklingsverksamhet* som närmare anges i 2 § sista strecksatsen och 3 § instruktionen. Myndigheten utför matematiska bedömningar av kryptosystem för totalförsvaret och biträder andra myndigheter vid värdering, utveckling, anskaffning och drift av signalspaningssystem. Vid utveckling av teknik och nya metoder för signalspaning är det ofta nödvändigt att testa systemen i den miljö där de skall vara verksamma för att säkerställa att de fungerar, d.v.s. kan inhämta signaler. Innehållet i signalerna är därvid inte av något intresse. Vid test av signalspaningssystem finns ingen teknisk möjlighet att på förhand sortera ut viss information som undantas från behandlingen. Eftersom signalerna kan innehålla personuppgifter bör den behandling av dessa uppgifter som inhämtningen innefattar ges stöd i lagen. I denna promemoria föreslås därför att Försvarets radioanstalt skall få behandla personuppgifter för detta ändamål. Av utvecklingsverksamhetens karaktär följer att det inte finns något intresse av att behandla dessa personuppgifter för andra ändamål, t.ex. i underrättelseverksamheten, eller att lämna ut dem till annan. Detta bör framgå av lagen. Vidare ligger det i sakens natur att uppgifter av aktuellt slag bör gallras efter kort tid. I enlighet med vad som anförs i avsnitt 8.20 bör den nödvändiga regleringen i denna del ske i förordning.

När det gäller uppgiften i instruktionen att utföra matematiska bedömningar av kryptosystem för totalförsvaret är denna verksamhet inte av sådan karaktär att motsvarande lagstöd är nödvändigt.

8.6 Personuppgifter som får behandlas inom den militära säkerhetstjänsten

8.6.1 Grunder för behandling i den militära säkerhetstjänsten av uppgifter om en person

Förslag: Uppgifter om en person får behandlas i den militära säkerhetstjänsten för de ändamål som anges i avsnitt 8.5 om

1. uppgifterna ger grundad anledning anta att personen utövat eller kan komma att utöva verksamhet som innefattar sådant hot mot rikets säkerhet som utgör brott eller terroristbrott enligt lagen (2003:148) om straff för terroristbrott eller motsvarande brottslighet enligt tidigare lagstiftning,

2. uppgifterna ger grundad anledning anta att personen utövat eller kan komma att utöva underrättelseverksamhet riktad mot Försvarmakten och dess säkerhetsintressen,

3. uppgifterna ger grundad anledning anta att personen utövar annan säkerhetshotande verksamhet än som avses i 1 och som innefattar brott eller åsidosättande av åligganden i anställning hos Försvarmakten, och det finns särskilda skäl till att uppgiften skall behandlas,

4. personen har lämnat uppgifter om säkerhetshotande verksamhet och personuppgifterna är nödvändiga för att bedöma personens trovärdighet, eller

5. uppgifterna avser information som har framkommit i samband med att en person har genomgått säkerhetsprövning enligt säkerhetsskyddslagen (1996:627).

Uppgifter om en person skall förse med upplysning om på vilken av de i första stycket angivna grunderna uppgiften behandlas. Om behandlingen av en personuppgift föranleds av annat än antagande om att personen har utövat eller kommer att utöva brottslig verksamhet skall det särskilt anges att personen inte är misstänkt för brottslig verksamhet, om det inte på annat sätt klart framgår att sådan misstanke inte finns. Uppgifter om en person som inte kan antas ha utövat eller komma att utöva annan säkerhetshotande verksamhet skall

förses med en särskild upplysning om detta, om det inte på annat sätt klart framgår att sådant antagande inte finns.

Uppgifter om en person som avses i punkterna 1–3 skall förses med en upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak.

Utredningens förslag överensstämmer i princip med promemorians men har en annorlunda redaktionell utformning. I promemorian föreslås vidare till skillnad från utredningens förslag att det skall framgå på vilken av de angivna grunderna behandling av personuppgifter sker samt att det särskilt skall anges om behandlingen varken föranleds av brottsmisstanke eller antagande om utövande av annan säkerhetshotande verksamhet.

Remissinstanserna tillstyrker eller har inte något att invända.

Skäl för förslaget: I avsnitt 8.5 lämnas förslag på de ändamål för vilka personuppgifter skall få behandlas inom den militära säkerhetstjänsten för att upptäcka, förebygga och avvärja säkerhetshot som riktas mot Försvarmakten och dess säkerhetsintressen. I detta avsnitt lämnas förslag på en särskild bestämmelse om de personer om vilka uppgifter får behandlas i verksamheten, som i princip motsvarar 14 § i förordningen (2001:703) om viss behandling av personuppgifter inom Försvarmakten och Försvarets radioanstalt. Den militära säkerhetstjänsten bedriver inte brottsutredande verksamhet, utan kommer in i ett skede före det att förundersökning inletts. Närmare beskrivning av verksamheten finns i avsnitt 3.1. I lagen bör närmare anges på vilka grunder uppgifter om en person får behandlas i den militära säkerhetstjänsten.

Här föreslås att uppgifter om en person skall få behandlas för de ändamål som anges i avsnitt 8.5 om uppgifterna ger grundad anledning anta att personen utövat eller kan komma att utöva verksamhet som innefattar sådant hot mot rikets säkerhet som utgör brott eller terroristbrott enligt lagen (2003:148) om straff för terroristbrott. Nämda lag trädde i kraft den 1 juli 2003, varför det i lagen bör anges att behandling av uppgifter får ske även

vid motsvarande brottslighet enligt tidigare lagstiftning, dvs. terrorism.

Hot mot rikets säkerhet kan aktualiseras även i samband med verksamhet som inte utgör brott. Uppgifter om en person skall därför kunna behandlas även när de ger grundad anledning att anta att en person utövat eller kommer att utöva underrättelseverksamhet mot Försvarsmakten och dess säkerhetsintressen.

Vidare skall uppgifter om en person få behandlas, om uppgifterna ger grundad anledning att anta att personen utövar annan säkerhetshotande verksamhet än den just angivna och som innefattar brott eller åsidosättande av åligganden in anställning hos Försvarsmakten och det finns särskilda skäl till att uppgiften skall behandlas. Också i detta avseende är det följaktligen möjligt att behandla personuppgifter även då personen inte kan antas utöva verksamhet som innefattar brott. Det finns nämligen behov av att i säkerhetstjänsten behandla uppgifter om en person även när den verksamhet som personen utövar endast hanteras disciplinärt. Kravet på särskilda skäl innebär dock att personuppgifter inte får behandlas vid en rent bagatellartad förseelse. Någon ytterligare omständighet erfordras för att behandling skall få ske. Som en grundläggande förutsättning gäller, enligt vad som framgår av avsnitt 8.5, att den säkerhetshotande verksamheten skall vara riktad mot Försvarsmakten och dess säkerhetsintressen.

Uppgifter om en person skall också få behandlas om personen har lämnat uppgifter om säkerhetshotande verksamhet och personuppgifterna är nödvändiga för att bedöma personens trovärdighet eller om uppgifterna har framkommit genom att någon genomgått en säkerhetsprövning enligt säkerhetsskyddslagen (1996:627).

När uppgifter behandlas i den militära säkerhetstjänsten är det av integritetsskäl viktigt att man särskiljer olika typer av uppgifter. Särskilt viktigt är det att det inte uppstår missuppfattningar om huruvida någon kan antas bedriva brottslig verksamhet eller inte. Det skall därför anges på vilken av de fyra angivna grunderna som behandlingen äger rum. När uppgifter behandlas om personer som inte misstänks för brott skall detta anges såvida det

inte klart framgår på annat sätt. Om det inte heller föreligger grund för antagande att personen har utövat eller kommer att utöva annan säkerhetsshotande verksamhet än sådan som innefattar brott skall också detta på motsvarande sätt anges, eftersom även sådana uppgifter får anses vara särskilt känslig ur integritetssynpunkt. Det är av mycket stor betydelse att denna typ av information fogas till personuppgiften eftersom den i ett senare skede minimerar att uppgiften övertolkas eller på annat vis kommer att värderas felaktigt.

Uppgifter som ger grundad anledning anta att en person bedriver säkerhetsshotande verksamhet skall förses med en upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak.

8.6.2 Signalkontrollverksamhet

Förslag: Personuppgifter som ingår i eller har uppkommit i samband med användning av totalförsvarets telekommunikations- och informationssystem får behandlas i den militära säkerhetstjänsten för att förhindra obehörig insyn i och påverkan av dessa system. Det gäller även känsliga personuppgifter och personnummer. Behandling som särskilt syftar till att identifiera en person får dock endast utföras om det finns grundad anledning att anta att det beträffande personen föreligger sådant antagande om att personen har utövat eller kommer att utöva säkerhetsshotande verksamhet som beskrivits i avsnitt 8.6.1.

Försvarmakten skall föra en förteckning över de behandlingar som särskilt syftar till att identifiera en person och de uppgifter som utgjort anledningen till behandlingen.

Utredningen har föreslagit att Försvarmaktens signalskyddstjänst skall undantas från bestämmelsen om vilka uppgiftskategorier som får behandlas i den militära säkerhetstjänsten.

Remissinstanserna tillstyrker eller har inte något att invända.

Skäl för förslaget: I den militära säkerhetstjänsten bedrivs signalkontroll för att förhindra obehörig insyn i och påverkan av totalförsvarets telekommunikations- och informationssystem. Sådan kontroll sker ofta rutinmässigt och måste förekomma utan föregående misstanke om samband med säkerhetshotande verksamhet. Kontrollen har till syfte att dels ge en bild av vad främmande signalspaning kan ha uppfattat av befordrad information, dels att kontrollera att totalförsvarets signalskyddssystem (kryptofunktioner) används och fungerar på önskat sätt. Signalkontrollen kan utöver innehållet i signalmeddelanden också avse om en teknisk utrustning avger oönskade signaler. Resultatet från en signalkontroll utnyttjas i första hand för att förbättra rutinerna vid meddelandeväxling. Signalkontroll avseende totalförsvarets telekommunikations- och informationssystem sker öppet, d.v.s. de som nyttjar systemen känner till att inhämtning av kommunikation kan förekomma.

Det är naturligt att det vid en signalkontroll behandlas personuppgifter av varierande slag. Det kan dels handla om direkta personuppgifter, t.ex. namn, som förekommer i utväxlade meddelanden, men också uppgifter som endast indirekt kan hänföras till en person, t.ex. uppgift om från vilken kommunikationsenhet ett meddelande härrör.

När en signalkontroll utförs är det inte möjligt att på förhand avgränsa vilka uppgifter som kommer att behandlas. Först efter att det insamlade materialet har bearbetats står det klart om det genom signalkontrollen har uppdagats någon säkerhetshotande verksamhet. Genom den föreslagna bestämmelsen klargörs att sådan behandling av personuppgifter i ett inledande skede kan genomföras, även såvitt avser känsliga personuppgifter och personnummer för vilka särskilt restriktiva bestämmelser gäller (se följande avsnitt). Bestämmelsen fyller följaktligen i detta avseende samma funktion som den av utredningen föreslagna.

När det vid en signalkontroll uppdagas säkerhetshotande verksamhet kan det finnas anledning att med utgångspunkt från den lagrade informationen vidta åtgärder för att identifiera en enskild person som kan vara upphovet till verksamheten. En be-

handling av personuppgifter i detta syfte skall endast få utföras när det finns grundad anledning att anta att personen har utövat någon sådan säkerhetshotande verksamhet som närmare beskrivits i föregående avsnitt. Ett exempel på när sådan behandling kan aktualiseras är när det vid en signalkontroll framkommer att en person – i regel en anställd i Försvarmakten – i ett meddelande som inte är skyddat av krypteringsfunktioner röjer en uppgift som omfattas av sekretess (se vidare avsnitt 3.1). Behandling för att identifiera och möjliggöra vidtagande av åtgärder mot personen kan då utföras med stöd av de bestämmelser som behandlas i avsnitt 8.6.1.

För att möjliggöra kontroll i efterhand av grunden för att en behandling utförts i syfte att identifiera en person skall Försvarmakten föra en förteckning över sådana behandlingar, av vilken skall framgå vilken person som avsetts med behandlingen och de uppgifter som utgjort anledningen till behandlingen. Innehållet i en sådan förteckning är naturligtvis känsligt ur integritetssynpunkt och bör därför gallras efter förhållandevis kort tid. I enlighet med vad som anförs i avsnitt 8.20 bör den nödvändiga regleringen i denna del ske i förordning.

8.7 Behandling av känsliga personuppgifter

Förslag: Uppgifter om en persons ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexualliv får behandlas endast såsom komplement till personuppgifter som behandlas på annan grund. Detta förutsätter att behandlingen är oundgängligen nödvändig med hänsyn till syftet med behandlingen. Uppgifter som beskriver en persons utseende skall alltid utformas på ett objektivt sätt med respekt för människovärdet.

Vid sökning skall sådana känsliga personuppgifter få användas som sökbegrepp endast om det är oundgängligen nödvändigt för syftet med behandlingen.

Utredningens förslag överensstämmer i princip med promemorians. Begränsningen av möjligheten att använda känsliga uppgifter som sökbegrepp föreslås av utredningen endast gälla vid sökning i uppgiftssamlingar.

De flesta remissinstanserna tillstyrker eller har inget att invända. *Säkerhetspolisen* anför att uppgifter om en person i polisens verksamhet får kompletteras med känsliga personuppgifter endast när det är oundgängligen nödvändigt för syftet med behandlingen. *Säkerhetspolisen* ifrågasätter varför det skall ställas strängare krav i polisens verksamhet än i försvarsunderrättelseverksamheten. *Registernämnden* anför att den under senare år iakttagit att den tekniska utvecklingen i fråga om datorer, som används inom *Säkerhetspolisen*, har medfört problem ifråga om tillåtlighet av behandling av personuppgifter. Användningen av fristående analysdatabaser synes enligt nämnden inte kunna ske utan att bestämmelserna i polisdatalagen om behandling av känsliga personuppgifter åsidosätts. Nämnden noterar att utredningens uppmärksammat motsvarande förhållanden när det gäller behandling av känsliga personuppgifter inom *Försvarsmakten* och *Försvarets radioanstalt*.

Skäl för förslaget: I 13 § personuppgiftslagen (1998:204) finns ett principiellt förbud mot behandling av känsliga personuppgifter. Med känsliga personuppgifter avses uppgifter om en person som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, eller som rör hälsa eller sexualliv. Personuppgiftslagen innehåller i 14–20 §§ en rad undantag från förbudet. I fråga om politiska åsikter stadgas dessutom i 2 kap. 3 § första stycket regeringsformen att anteckning om medborgare i allmänt register inte utan hans samtycke får grundas enbart på hans politiska åskådning.

Försvarsmakten och *Försvarets radioanstalt* har många gånger ett befogat intresse av att kunna registrera och på annat sätt behandla känsliga personuppgifter i de verksamheter som omfattas av denna promemoria. Det kan t.ex. vara nödvändigt inom ramen för Sveriges deltagande i internationella fredsbevarande och hu-

manitära insatser. I dessa uppdrag ingår ofta att skydda en viss minoritet. För att de svenska enheterna inom en sådan mission skall kunna utföra sina uppgifter kan det därför vara nödvändigt att uppgifter behandlas rörande t.ex. etnisk härkomst eller religiös övertygelse. Här bidrar såväl den militära underrättelse- och säkerhetstjänsten som Försvarets radioanstalt med underrättelser. Även i övrigt finns det ett behov av att kunna behandla känsliga personuppgifter. Ofta är just det faktum att en person tillhör ett politiskt parti eller annan organisation av grundläggande betydelse från försvarsunderrättelse- eller säkerhetstjänstsynpunkt. En sådan omständighet får dock aldrig utgöra ensam grund för behandlingen. Det ligger således i verksamhetens natur att denna typ av uppgifter kan ha en betydelse för resultatet av den slutliga analysen.

Säkerhetspolisen har påtalat att polisen får komplettera uppgifter om en person med känsliga personuppgifter endast när det är oundgängligen nödvändigt för syftet med behandlingen. Motsvarande gäller för brottsbekämpande verksamhet inom Tullverket, Skatteverket och Kustbevakningen. Den svenska regleringen har i dessa hänseenden sin grund i Europarådets rekommendation No. R(87)15 om användning av personuppgifter inom polissektorn. Bakgrunden till rekommendationen var att Europarådet, mot bakgrund av ökad polisiär verksamhet med anledning av nya hot som terrorism och ökad brottslighet, ansåg det särskilt angeläget att för polissektorn meddela tydliga riktlinjer. Avsikten var att genom riktlinjerna peka på en nödvändig avvägning mellan å ena sidan enskilda människors rättigheter och å andra sidan rättmätig polisiär verksamhet (se vidare Europarådets "explanatory memorandum" på www.coe.int). Begränsningen till behandling som är oundgängligen nödvändig gäller även viss behandling av personuppgifter som inte omfattas av Europarådets rekommendation, t.ex. inom kriminalvården och i verksamhet enligt utlännings- och medborgarskapslagstiftningen.

Det ligger i sakens natur att i den verksamhet som regleras i de nu lämnade lagförslagen är just uppgifter om etniskt ursprung, politiska åsikter och religiös övertygelse sådana faktorer som är

av stor betydelse när det gäller att bedöma personers eller grupperns agerande i ett ur försvarsunderrättelseperspektiv relevant avseende. Inte minst gäller detta vid försvarsunderrättelseverksamhet till stöd för svenska militära operationer utomlands, då konflikterna ofta har sitt ursprung i etniska, politiska eller religiösa motsättningar. Självklart måste dock även i de nu aktuella verksamheterna stor försiktighet iakttas med avseende på behandling av känsliga personuppgifter. Att möjligheten att behandla sådana personuppgifter skall användas mycket restriktivt bör framgå genom att det i lagarna anges att sådan behandling får äga rum endast då det är oundgängligen nödvändigt för verksamheten. I denna promemoria föreslås därför att Försvarsmakten respektive Försvarets radioanstalt skall få behandla känsliga personuppgifter om en person endast om uppgifterna kompletterar personuppgifter som behandlas på annan grund. Därutöver skall det krävas att behandlingen av känsliga personuppgifter är oundgängligen nödvändig för syftet med behandlingen. Detta innebär exempelvis att det inte är tillåtet att i underrättelseverksamhet föra register över, eller på annat sätt göra anteckningar om, enskilda personer enbart på den grunden att de tillhör en viss etnisk grupp. Uppgifter som beskriver en persons utseende skall alltid utformas på ett objektiva sätt med respekt för människovärdet. Detta bör framgå direkt av lagtexten.

Automatiserad behandling av personuppgifter, i synnerhet i samlingar av uppgifter, ger stora möjligheter att söka och sammanställa information. Dessa möjligheter medför särskilt stora risker för intrång i den personliga integriteten. I syfte att begränsa denna risk finns det anledning att överväga en begränsning av sökmöjligheterna. Samtidigt måste beaktas att just möjligheten att enkelt och snabbt söka information skapar förutsättningar för en rationell verksamhet. Eventuella begränsningar får därför inte vara så snäva att de medför onödiga effektivitetsförluster.

Behovet av rättsliga begränsningar av vilka uppgifter som skall få användas vid sökning gör sig framförallt gällande i fråga om känsliga personuppgifter. I konsekvens med de grundläggande kraven för behandling av känsliga personuppgifter bör sökning

efter information om känsliga personuppgifter endast få ske om det är oundgängligen nödvändigt för syftet med behandlingen. Det innebär att en uppgift om t.ex. etnisk härkomst får användas som sökbegrepp bara under den förutsättningen att det är oundgängligen nödvändigt för att få fram den information som behövs för att t.ex. utföra en fredsbevarande eller humanitär insats som åligger svenskt förband eller annan organisationsenhet.

Bestämmelsen om behandling av känsliga personuppgifter och sökning med sådana uppgifter skall vara generell, dvs. den bör gälla såväl för behandling i Försvarmaktens och Försvarets radioanstalts olika uppgiftssamlingar som för annan behandling.

Registernämndens remissynpunkt behandlas i avsnitt 8.9.

8.8 Behandling av personnummer

Förslag: Uppgifter om personnummer eller samordningsnummer får behandlas bara när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl.

Utredningen har inte lämnat något motsvarande förslag.

Skäl för förslaget: Enligt dataskyddsdirektivet skall medlemsstaterna bestämma på vilka villkor ett nationellt identifikationsnummer eller något annat vedertaget sätt för identifiering får behandlas. En reglering av användande av personnummer finns således i 22 § personuppgiftslagen (1998:204). Där anges att uppgifter om personnummer eller samordningsnummer får behandlas bara när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl. Personnummer eller samordningsnummer får därutöver behandlas om den enskilde ger sitt samtycke till det.

En liknande bestämmelse bör av integritetsskäl införas i de båda lagförslagen om personuppgiftsbehandling. Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst respektive Försvarets radioanstalts underrättelse- och ut-

vecklingsverksamhet baserar sig inte på samtycke från den enskilde. Om behandlingen av personnummer eller samordningsnummer inte är klart motiverad med hänsyn till dess ändamål, till vikten av en säker identifiering eller något annat beaktansvärt skäl skall den inte förekomma.

Bestämmelsen skall vara generell, dvs. den bör gälla såväl för behandling i Försvarmaktens och Försvarets radioanstalts olika uppgiftssamlingar som för annan behandling.

8.9 Behandling av personuppgifter i vissa fall

Förslag: Försvarets radioanstalts behandling av personuppgifter som innebär inhämtning av personuppgifter genom signalspaning, lagring av uppgifter som sker omedelbart därefter och bearbetning i form av kryptoforcering och språklig översättning skall inte anses som oförenlig med bestämmelserna om grundläggande krav, ändamål samt behandling av känsliga personuppgifter och personnummer.

Utredningen har inte lämnat något motsvarande förslag.

Skäl för förslaget: Som redovisats i avsnitt 8.7 har Registernämnden anfört att utredningen har uppmärksammat frågan om hur bestämmelsen om känsliga personuppgifter förhåller sig till den information som Försvarets radioanstalt inhämtar genom signalspaning. Utredningens uppfattning är att inhämtning av okänd information genom signalspaning inte strider mot bestämmelsen om behandling av känsliga personuppgifter. Utredningen anför att bestämmelsen måste tillämpas på varje enskild behandling för sig och att inhämtning genom signalspaning är en sådan enskild behandling. Vid denna inhämtning finns överhuvudtaget inget syfte att behandla känsliga personuppgifter, eftersom informationen i detta led av processen ännu är helt okänd.

Här uppmärksammas frågan om behandlingens laglighet i ett bredare perspektiv. Försvarets radioanstalt behandlar en mycket stor mängd information som inhämtas genom signalspaning (angående begreppet signalspaning, se avsnitt 4.1). Inhämtningen

sker endast för att Försvarets radioanstalt skall uppfylla sin grundläggande uppgift att genom signalspaning bedriva under rättelse- och utvecklingsverksamhet. Inhämtning av signaler sker såväl manuellt utan urval som automatiskt med särskilda sökbegrepp. Oavsett hur inhämtningen sker tillförs Försvarets radioanstalt stora mängder obearbetad information. I informationen kan det dölja sig uppgifter om enskilda personer och också känsliga personuppgifter och personnummer. Försvarets radioanstalt har utöver den begränsning av inhämtningen som användandet av sökbegrepp innebär liten möjlighet att påverka innehållet i den information som inhämtas. I princip inhämtas all den information som träffas av sökbegreppen, oavsett dess relevans för verksamheten. Det är följaktligen okänt för Försvarets radioanstalt vid själva inhämtningen och den efterföljande lagringen vad den inhämtade informationen innehåller. Därtill kommer att informationen ofta är såväl krypterad som avfattad på ett främmande språk. Det är i detta skede således inte möjligt för myndigheten att "censurera" innehållet i information som på detta sätt kommer in i elektronisk form genom att ta bort t.ex. känsliga personuppgifter. Det är först sedan de inhämtade signalerna lagrats och därefter bearbetats genom att signalskyddet forcerats och informationen översatts som informationen kan tas fram i klartext eller sändningarnas innehåll kan beskrivas. Det är då myndigheten får klart för sig om det insamlade materialet innehåller personuppgifter och om det även är fråga om t.ex. känsliga personuppgifter.

Med hänsyn till att de inhämtade signalerna således utan Försvarets radioanstalts vetskap kan innehålla personuppgifter, kan fråga uppkomma om myndigheten i ett initialt skede kan anses behandla dessa personuppgifter enligt de regler om ändamål m.m. som föreslås här. I denna promemoria föreslås därför en förtydligande bestämmelse om att Försvarets radioanstalts behandling av personuppgifter som innebär inhämtning av personuppgifter genom signalspaning, lagring av uppgifter som sker omedelbart därefter och bearbetning i form av kryptoforcering och språklig översättning inte skall anses som oförenlig med be-

stämmelserna om grundläggande krav, ändamål samt behandling av känsliga personuppgifter och personnummer i det skede av behandlingen under vilket det ännu inte kunnat fastställas om den inhämtade, lagrade eller bearbetade informationen innehåller personuppgifter. Först sedan uppgifterna bearbetats genom kryptoforcering och språklig översättning kan Försvarets radioanstalt konstatera om det är fråga om personuppgifter. Därefter får inte ytterligare personuppgiftsbehandling, som t.ex. vidare bearbetning eller lagring, ske utan att behandlingen överensstämmer med de bestämmelser som föreslås här.

8.10 Överföring av personuppgifter till andra länder

Förslag: Försvarmakten respektive Försvarets radioanstalt får föra över personuppgifter till andra länder om sekretess inte hindrar det. Som en ytterligare förutsättning gäller att överföringen av uppgifter är nödvändig för att myndigheten skall kunna fullgöra sina uppgifter inom ramen för det internationella försvarsunderrättelse- och säkerhetssamarbetet.

Regeringen får föreskriva eller i särskilt fall besluta om att överföring även får ske i andra fall om det är nödvändigt för att Försvarmakten eller Försvarets radioanstalt skall kunna fullgöra sina uppgifter.

Utredningens förslag överensstämmer delvis med promemorians. I utredningens förslag till rubrik – dock inte i paragrafen – används begreppet tredje land. Utredningen föreslår vidare att personuppgifter skall få överlämnas även när det annars är nödvändigt för verksamheten. Utredningens förslag saknar möjlighet för regeringen att föreskriva om utlämnande i vissa fall.

Remissinstanserna tillstyrker eller har inte något att invända. *Göteborgs universitet* anser emellertid att utredningens förslag ger Försvarmakten och Försvarets radioanstalt en allt för stor frihet utan någon överprövning före utlämnandet. Universitet

föreslår att myndigheterna skall ha ett särskilt skriftligt tillstånd för varje utlämnande av personuppgifter till ett annat land.

Skäl för förslaget: Det är enligt 33 § personuppgiftslagen (1998:204) förbjudet att till tredje land föra över personuppgifter som är under behandling om landet inte har en adekvat nivå för skyddet av personuppgifter. Med tredje land avses, enligt 3 §, en stat som inte ingår i Europeiska unionen eller är ansluten till Europeiska ekonomiska samarbetsområdet. Från förbudet finns vissa undantag i 34 §, bl.a. för överföring till länder som har anslutit sig till Europarådets dataskyddskonvention. Enligt 35 § andra stycket har regeringen eller den myndighet som regeringen bestämmer möjlighet att föreskriva om undantag från förbudet, om det behövs med hänsyn till ett viktigt allmänt intresse eller om det finns tillräckliga garantier till skydd för de registrerades rättigheter.

Bestämmelser om överföring av personuppgifter till andra länder finns även i Europarådets dataskyddskonvention, genom ett tilläggsprotokoll som Sverige undertecknade den 8 november 2001. Enligt artikel 2 första punkten i tilläggsprotokollet skall varje part endast möjliggöra överföring av personuppgifter till en mottagare som lyder under en stats eller en organisations jurisdiktion och som inte är part i konventionen, om staten eller organisationen tryggar en tillräcklig grad av skydd för den avsedda uppgiftsöverföringen. Som undantag från första punkten får en part tillåta överföring om det är tillåtet enligt den nationella lagstiftningen på grund av den registrerades särskilda intressen, eller när legitima intressen överväger, i synnerhet viktiga allmänna intressen.

Utlämnande av uppgifter till andra länder kan för Försvarsmaktens och Försvarets radioanstalts del behöva ske inom ramen för det internationella försvarsunderrättelse- och säkerhetssamarbetet. Av 3 § lagen (2000:130) om försvarsunderrättelseverksamhet och 3 § den därtill hörande förordningen framgår att Försvarsmakten och Försvarets radioanstalt under vissa förutsättningar får, enligt regeringens bestämmande, samarbeta i underrättelsefrågor med andra länder. I Ds 2005:30 En anpassad

försvarsunderrättelseverksamhet föreslås att Försvarets radioanstalt även för övrig underrättelseverksamhet under vissa förutsättningar får, enligt regeringens närmare bestämmande, samarbeta med andra länder och organisationer (se avsnitt 6). Utlands-samarbete är också för den militära säkerhetstjänsten en naturlig del av verksamheten. Som framgår av avsnitt 3.1 anges i regleringsbrevet för budgetåret 2005 att samarbete med andra länder är en naturlig del av den militära säkerhetstjänsten och att utbyte av information anses nödvändigt för att Sverige skall kunna få del av sådan information som landet behöver men som kräver resurser som saknas.

Av 5 § förordningen (2001:703) om viss behandling av personuppgifter inom Försvarsmakten och Försvarets radioanstalt framgår att uppgifter får lämnas ut till en utländsk myndighet eller en internationell organisation, om utlämnandet tjänar den svenska statsledningen eller det svenska totalförsvaret. De uppgifter som Försvarsmakten eller Försvarets radioanstalt lämnar till andra länder och internationella organisationer får enligt samma bestämmelse dock inte vara till skada för svenska intressen.

Sveriges allt bredare medverkan i det internationella försvarsunderrättelse- och säkerhetssamarbetet kräver att statsmakterna genom underrättelsetjänsten får erforderlig information att lägga till grund för konfliktförebyggande åtgärder, krishantering, planering och beslut om insats. Vidare krävs att information kan lämnas som stöd för insatsstyrkornas säkerhet och operationer i missionsområdet. Underrättelsefunktionen är en förutsättning för styrkornas säkerhet, för deras förmåga att lösa sina uppgifter, för kontroll av bevakningsområdet och för att kunna leda lokala förhandlingar. I krislägen då internationella insatser övervägs krävs också snabba konsultationer mellan alla de stater och organisationer som överväger att delta (jfr. prop. 2001/02:10 s. 245 f.).

Mot ovanstående bakgrund framgår att det är av stor betydelse att uppgifter kan utbytas med andra länder även om det medför en överföring av personuppgifter till ett tredje land enligt per-

sonuppgiftslagen eller till en mottagare som inte är part i dataskyddskonventionen. Möjligheten att inom det internationella försvarsunderrättelse- och säkerhetssamarbetet utbyta uppgifter med andra länder utgör ett sådant legitimt allmänt intresse som avses i dataskyddskonventionen. I de föreslagna lagarna skall därför finnas en bestämmelse som medger att personuppgifter förs över till ett annat land. Överföring av personuppgifter skall dock endast få ske om sekretess inte hindrar det och det är nödvändigt för att Försvarmakten respektive Försvarets radioanstalt skall kunna fullgöra sina uppgifter inom ramen för det internationella försvarsunderrättelse- och säkerhetssamarbetet. Vid utlämnande av uppgifter till utlandet tillämpar såväl Försvarmakten som Försvarets radioanstalt stränga säkerhetskrav för att skydda sin egen verksamhet. De bestämmelser om sekretess och krav på säkerhet som gäller för verksamheterna tillgodoser skyddet för den personliga integriteten i tillräcklig mån.

Bestämmelsen i 5 § förordningen (2001:703) om viss behandling av personuppgifter inom Försvarmakten och Försvarets radioanstalt motsvarar 3 § förordningen (2000:131) om försvarsunderrättelseverksamhet och avses få sin motsvarighet också i den förordning som skall meddelas i anslutning till den föreslagna lagen om signalspaning (se kap. 6). Det är därför av systematiska skäl inte lämpligt att överföra denna bestämmelse direkt till lagarna, utan en sådan reglering bör också i nu aktuellt avseende ske i förordning (se vidare avsnitt 8.21.1).

De krav som ställs för överföring av personuppgifter gäller i förhållande till alla länder. Det kan därför övervägas om bestämmelsen skall begränsas till att endast omfatta överföring till tredje land. Personuppgiftslagens reglering om överföring av personuppgifter till tredje land grundas på bestämmelser i dataskyddsdirektivet. Med tredje land avses en stat som inte ingår i Europeiska unionen eller är ansluten till Europeiska ekonomiska samarbetsområdet (EES) och följaktligen inte är bunden av direktivet och därmed inte kan förutsättas ha en adekvat skyddsnivå. Som redogjorts för i avsnitt 5.1.2 och 5.1.3 omfattas inte behandling av personuppgifter i Försvarmaktens försvarsunderrät-

telseverksamhet och militära säkerhetstjänst samt i Försvarets radioanstalts underrättelseverksamhet av dataskyddsdirektivet. I fråga om sådana personuppgifter som de nu föreslagna lagarna reglerar saknar det alltså betydelse om utlämnande sker till ett land som omfattas av dataskyddsdirektivet eller till ett tredje land i personuppgiftslagens mening. Det framstår därför som mindre lämpligt att i de föreslagna lagarna använda begreppet tredje land med den definition som ges i personuppgiftslagen.

Till skillnad från dataskyddsdirektivet är dataskyddskonventionen tillämplig även i fråga om sådan verksamhet som regleras av de föreslagna lagarna. En möjlighet vore därför att här definiera tredje land som en stat som inte omfattas av denna konvention. Mot bakgrund av att begreppet tredje land redan har en legal definition bör det dock inte i de föreslagna lagarna ges en annan innebörd. Eftersom de angivna förutsättningarna för överföring av personuppgifter är relevanta i förhållande till alla länder saknas det också anledning att på annat sätt ange en begränsning av bestämmelsens tillämplighet till stater som inte omfattas av dataskyddskonventionen. Med den föreslagna lydelsen uppfyller bestämmelserna i vart fall de krav dataskyddskonventionen ställer på nationell lagstiftning i fråga om överföring av personuppgifter till andra länder.

Det internationella samarbetet befinner sig i en dynamisk utveckling. Det är omöjligt att förutse när eller på vilket sätt som uppgifter i de aktuella verksamheterna behöver sändas till andra länder. Därför föreslås här en möjlighet för regeringen att genom föreskrifter eller särskilt beslut få bestämma att utlämnande även skall få ske i andra fall om det är nödvändigt för att Försvarmakten eller Försvarets radioanstalt skall kunna fullgöra sina uppgifter. Bemyndigandet för regeringen motiveras av att det exempelvis vid ett förband i utlandsstyrkan inom Försvarmakten i vissa situationer är nödvändigt att överlämna underrättelser till ett organ i en annan stats väpnade styrkor som inte kan sägas vara ett underrättelse- eller säkerhetsorgan.

Goteborgs universitet har föreslagit att utlandssamarbete som innefattar utlämnande av personuppgifter skall föregås av ett

skriftligt tillstånd. Det utlandssamarbete som bedrivs och föreslås bedrivs sker enligt regeringens närmare bestämmande (se ovan). Försvarsmakten och Försvarets radioanstalt skall till Regeringskansliet anmäla frågor om att etablera och upprätthålla sådant samarbete samt lämna information om viktiga frågor som uppkommer, 4 § förordningen (2000:131) om försvarsunderrättelseverksamhet. Myndigheterna skall också informera Försvarets underrättelsenämnd, som utövar tillsyn över försvarsunderrättelseverksamheten, om de principer som tillämpas för samarbetet samt lämna uppgift om med vilka länder och organisationer som samarbete sker. Myndigheterna skall vidare sedan samarbetet etablerats informera nämnden om omfattningen av samarbete och, när det bedöms påkallat, om resultatet, erfarenheterna och den fortsatta inriktningen av samarbete, 6 § nämnda förordning. I Ds 2005:30 En anpassad försvarsunderrättelseverksamhet föreslås att nämnden skall kontrollera även inhämtningen enligt den föreslagna signalspaningslagen. Dessa bestämmelser i förening med den nu föreslagna bestämmelsen om överföring av personuppgifter till andra länder begränsar Försvarsmaktens och Försvarets radioanstalts möjligheter att bedriva samarbete med andra länder i tillräcklig grad.

8.11 Information till den enskilde

Förslag:

Information skall lämnas självmant

När uppgifter om en person samlas in i den militära säkerhetstjänsten från personen själv skall Försvarsmakten i samband därmed lämna denne information om behandlingen av uppgifterna. Informationen skall omfatta bl.a. uppgift om ändamålen med behandlingen och all övrig information som behövs för att den om vilken uppgifter behandlas skall kunna ta till vara sina rättigheter i samband med behandlingen. Infor-

mationen behöver inte lämnas om sådant som denne redan känner till.

Information skall lämnas efter ansökan

Försvarsmakten och Försvarets radioanstalt är skyldiga att till var och en som ansöker om det en gång per kalenderår gratis lämna besked om personuppgifter som rör den sökande behandlas eller inte. Om sådana uppgifter behandlas skall skriftlig information lämnas också om bl.a. vilka uppgifter som behandlas och ändamålen med behandlingen.

Information skall lämnas inom en månad från det att ansökan gjordes. Om det finns särskilda skäl för det, får information dock lämnas senast fyra månader efter det att ansökan gjordes.

Information behöver inte lämnas i den utsträckning detta visar sig vara omöjligt eller skulle innebära en oproportionerligt stor arbetsinsats. Information behöver inte heller lämnas om personuppgifter i löpande text som inte fått sin slutliga utformning när ansökan gjordes eller som utgör minnesanteckning eller liknade. Detta gäller dock inte om uppgifterna har lämnats ut till tredje man eller, när det gäller löpande text som inte fått sin slutliga utformning, om uppgifterna har behandlats under längre tid än ett år.

Undantag från informationsskyldigheten

Undantag från informationsskyldigheten skall göras vid sekretess.

Utredningens förslag överensstämmer delvis med promemoriernas. Utredningen föreslår att Försvarsmakten och Försvarets radioanstalt självmant skall lämna den registrerade information om personuppgiftsbehandling även när uppgifter om en person samlas in från personen själv i Försvarsmaktens försvarsunder-

rättelseverksamhet respektive i Försvarets radioanstalts underrättelse- och utvecklingsverksamhet.

Remissinstanserna tillstyrker eller har inte något att invända. *Göteborgs universitet* föreslår att det införs en bestämmelse om underrättelse till den registrerade i efterhand. En vetskap om att den registrerade i efterhand skall få kännedom om det som beslutats och registrerats medför, enligt universitetet, att den prövning som skall göras sker på ett mer ansvarsfullt sätt.

Skäl för förslaget: I 23–27 §§ personuppgiftslagen (1998:204) finns bestämmelser om den personuppgiftsansvariges skyldighet att lämna information till den registrerade. Bestämmelserna reglerar två olika situationer. Den första situationen avser det fall att personuppgifter samlas in från personen själv eller från någon annan källa. Den personuppgiftsansvarige skall i dessa fall lämna den registrerade information självmant. Olika regler gäller dock beroende på om personuppgifterna samlas in från den registrerade själv eller om de samlas in från någon annan, 23–25 §§. Den andra situationen gäller när den enskilde ansöker om att få besked om personuppgifter som rör denne behandlas eller inte. Den personuppgiftsansvarige skall i dessa fall lämna information inom viss tid. Visst undantag görs för personuppgifter i löpande text, 26 §. I båda situationerna gäller att bestämmelser om sekretess och tystnadsplikt alltid går före informationsskyldigheten, 27 §.

Information skall lämnas självmant

Den information som den personuppgiftsansvarige enligt personuppgiftslagen självmant skall lämna en enskild då personuppgifter samlats in från den enskilde själv skall omfatta uppgifter om den personuppgiftsansvariges identitet, ändamålen med behandlingen samt övrig information som behövs för att den registrerade skall kunna ta till vara sina rättigheter, 23 och 25 §§. Information behöver inte lämnas om sådant som den registrerade redan känner till. Denna informationsskyldighet förutsätter att personuppgifter samlas in från den registrerade vid någon form

av direktkontakt med denne. I den militära säkerhetstjänsten samlas personuppgifter till viss del in vid direktkontakt med den registrerade. Självfallet erhåller den militära säkerhetstjänsten tydligare och mer fullständiga uppgifter om uppgiftslämnaren känner ett förtroende för den som skall ha uppgiften. Likaså ökar samarbetsviljan om uppgiftslämnaren förstår vikten av att uppgiften lämnas. En informationsbestämmelse motsvarande den i 23 och 25 §§ personuppgiftslagen skall därför gälla vid behandling av personuppgifter inom den militära säkerhetstjänsten.

När det gäller behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och i Försvarets radioanstalts underrättelse- och utvecklingsverksamhet är situationen en annan. Försvarsunderrättelseverksamheten skall avse utländska förhållanden och bedrivs till stöd för svensk utrikes-, säkerhets- och försvarspolitik. Verksamheterna är av sådan art att en motsvarande skyldighet för myndigheterna att lämna information inte är realistisk. Härtill kommer för Försvarets radioanstalts del att myndigheten bedriver underrättelse- och utvecklingsverksamhet genom signalspaning, dvs. genom att myndigheten med mottagarsystem och andra elektroniska hjälpmedel registrerar telesändningar och signaler. Uppgifter inhämtas inte direkt från den registrerade. I denna promemoria föreslås därför inte någon motsvarande informationsbestämmelse såvitt avser behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och i Försvarets radioanstalts underrättelse- och utvecklingsverksamhet.

Om personuppgifter har samlats in från någon annan källa än den registrerade skall, enligt 24 § personuppgiftslagen, den personuppgiftsansvarige självmant lämna den registrerade information om behandlingen av uppgifterna när de registreras. Informationen behöver dock inte lämnas om det finns bestämmelser om registrerandet eller utlämnandet av personuppgifter i en lag eller någon författning.

Frågan om behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst samt Försvarets radioanstalts underrättelse- och utvecklings-

verksamhet regleras i de här föreslagna lagarna och i de förordningar som kommer att utarbetas. Den registrerade kan således genom att läsa bestämmelserna få klart för sig på vilket sätt personuppgifterna behandlas i dessa verksamheter. Det saknas därför anledning att föreslå en bestämmelse med motsvarande innehåll.

Information skall lämnas efter ansökan

Enligt 26 § personuppgiftslagen har enskilda rätt att efter ansökan få information av den personuppgiftsansvarige om personuppgifter som rör den registrerade behandlas eller inte. Om uppgifter behandlas skall information lämnas om vilka uppgifter det rör sig om, varifrån uppgifterna har hämtats, ändamålen med behandlingen och till vilka mottagare eller kategorier av mottagare som uppgifterna har lämnats ut. Ansökan skall göras skriftligen hos den personuppgiftsansvarige och vara undertecknad av den sökande själv. Information skall lämnas inom en månad från det att ansökan gjordes. Om det finns särskilda skäl för det, får information dock lämnas senast efter fyra månader. Information behöver emellertid inte lämnas beträffande personuppgifter som behandlas endast i löpande text som ännu inte fått sin slutliga utformning eller som utgör minnesanteckningar, under förutsättning att uppgifterna inte har lämnats ut till tredje man.

Personuppgiftslagsutredningen föreslår i sitt betänkande SOU 2004:6 Översyn av personuppgiftslagen att information enligt 26 § personuppgiftslagen inte skall behöva lämnas i den utsträckning detta visar sig vara omöjligt eller skulle innebära en oproportionerligt stor arbetsinsats. Om den personuppgiftsansvarige bara efter väldigt stora ansträngningar kan få fram uppgifter om en person, är det, enligt utredningens mening, mindre sannolikt att dessa uppgifter kommer att användas på ett sätt som innebär ett otillbörligt intrång i den personliga integriteten (se betänkandet s. 195). Utredningens förslag är föremål för beredning i Regeringskansliet.

Även vid personuppgiftsbehandling i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst respektive i Försvarets radioanstalts underrättelse- och utvecklingsverksamhet är det angeläget att varje registrerad har rätt att efter begäran få viss information från myndigheterna. I denna promemoria lämnas därför förslag på en bestämmelse motsvarande den i 26 § personuppgiftslagen. Därutöver bör en bestämmelse liknande den som Personuppgiftslagsutredningen föreslår gälla.

Goteborgs universitet föreslår att Försvarmakten och Försvarets radioanstalt i efterhand skall underrätta den registrerade. Detta skulle, enligt universitetets mening, få till följd att den prövning som skall göras av respektive myndighet sker på ett mer ansvarsfullt sätt. Som anförts tidigare är Försvarmaktens försvarsunderrättelseverksamhet och Försvarets radioanstalts underrättelse- och utvecklingsverksamhet av sådan art att det med hänsyn till verksamheterna inte är möjligt att ålägga myndigheterna en skyldighet att självmant informera den enskilde om behandling som äger rum. Samma överväganden gör sig gällande här. För att förstärka skyddet för den personliga integriteten vid behandling av personuppgifter inom dessa verksamheter föreslås att en särskild granskning till skydd för integriteten skall ske, se avsnitt 8.16.

Undantag från informationsskyldigheten

Många uppgifter som behandlas i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst samt i Försvarets radioanstalts underrättelse- och utvecklingsverksamhet är hemliga såväl med hänsyn till Sveriges förhållande till främmande makt som till skydd för rikets säkerhet, 2 kap. 1–2 §§ sekretesslagen (1980:100). Det är också viktigt att skydda uppgiftslämnare och arbetsmetoder. Den informationsskyldighet som föreslås i detta avsnitt skall därför, på motsvarande sätt som anges i 27 § personuppgiftslagen, inte gälla i den utsträckning sekretess hindrar att uppgifterna lämnas ut till den registrerade.

Bestämmelserna om enskildas rätt till information hör till de viktigaste medlen för att personuppgifter inte skall behandlas på ett sätt som kan medföra att enskildas personliga integritet kränks. Den sekretess som gäller för uppgifter i de verksamheter som regleras i denna promemoria innebär emellertid att information sällan kommer att lämnas av myndigheterna. Utan kunskap om vilka uppgifter som behandlas kommer den enskilde inte att kunna kontrollera att uppgifter om honom eller henne behandlas korrekt och i enlighet med vad som är särskilt föreskrivet. Mot denna bakgrund lämnas i avsnitt 8.16 förslag om att en särskild granskning till skydd för den personliga integriteten skall äga rum. Bestämmelser om information fyller dock en viktig funktion i de fall där sekretess inte gäller för uppgifterna.

8.12 Rättelse

Förslag: Försvarsmakten och Försvarets radioanstalt skall på begäran av den registrerade snarast rätta, blockera eller utplåna sådana personuppgifter som inte har behandlats i enlighet med respektive lag eller föreskrifter som har utfärdats med stöd av lagen.

Myndigheterna skall också underrätta tredje man till vilken uppgifterna har lämnats ut om åtgärden, om den registrerade begär det eller om mera betydande skada eller olägenhet för den registrerade skulle kunna undvikas genom en underrättelse. Någon sådan underrättelse behöver dock inte lämnas, om detta visar sig vara omöjligt eller skulle innebära en oproportionerligt stor arbetsinsats.

Utredningen förslår att det i en bestämmelse skall anges att bestämmelserna om rättelse i personuppgiftslagen (1998:204) skall gälla vid behandling av personuppgifter enligt lagförslagen.

Remissinstanserna tillstyrker eller har inte något att invända. *Kammarrätten i Stockholm* påtalar att juridiska personer inte kommer att omfattas av en lagreglerad rätt till rättelse genom

den av utredningen föreslagna hänvisningen till personuppgiftslagen vad gäller rätten till rättelse av felaktiga uppgifter.

Skäl för förslaget: Den personuppgiftsansvarige är, enligt 28 § personuppgiftslagen, skyldig att på begäran av den registrerade rätta, blockera eller utplåna sådana personuppgifter som inte behandlats i enlighet med lagen eller föreskrifter meddelade med stöd av lagen. Den personuppgiftsansvarige har även, med vissa undantag, en skyldighet att underrätta tredje man till vilken uppgifterna lämnats ut om korrigeringsåtgärden.

Att en personuppgift rättas innebär att den ersätts eller kompletteras med korrekta uppgifter. Med blockering avses en åtgärd som vidtas för att personuppgifter skall vara förknippade med information om att de är spärrade och om anledningen till spärran. Att en uppgift utplånas innebär att den förstörs så att den inte kan återskapas.

Det är av väsentlig betydelse för den enskilde att personuppgifter som behandlas felaktigt hos Försvarmakten eller Försvarets radioanstalt rättas för att intrång i den personliga integriteten skall undvikas. Bedömningen av om en uppgift har behandlats felaktigt måste göras mot bakgrund av de bestämmelser som gäller för behandlingen. En bestämmelse som ger den enskilde rätt att, på motsvarande sätt som gäller enligt 28 § personuppgiftslagen, påkalla Försvarmaktens eller Försvarets radioanstalts aktivitet för att korrigera uppgifter skall därför tillämpas vid behandling av personuppgifter enligt de föreslagna författningarna. Försvarmakten och Försvarets radioanstalt har redan på grundval av förslaget till grundläggande krav på behandling av personuppgifter skyldighet att på eget initiativ korrigera felaktiga personuppgifter (se avsnitt 8.4).

Lagförslagen omfattar inte, till skillnad mot utredningens förslag, behandling av uppgifter om juridiska personer. Se övervägandena i denna del i avsnitt 7.3.

8.13 Skadestånd

Förslag: Staten skall ersätta den registrerade för skada och kränkning av den personliga integriteten som en behandling av personuppgifter i strid med de föreslagna lagarna har orsakat. Ersättningsskyldigheten skall i den utsträckning det är skäligt jämkas, om Försvarsmakten och Försvarets radioanstalt visar att felet inte berodde på myndigheten.

Utredningens förslag överensstämmer med promemorians.

Remissinstanserna tillstyrker eller har inte något att invända. *Göteborgs universitet* föreslår att preskriptionsregler för rätten till skadestånd i anledning av brott införs så att preskriptionstiden räknas från den tidpunkt den skadelidande får kännedom om den skadebringande handlingen och inte, som normalt, från tidpunkten då den skadebringande handlingen företogs. Universitetet menar att skadeståndsrätten annars blir utan verkan eftersom den skadelidande kanske får kännedom om den skadebringande handlingen först lång tid efter det att handlingen vidtogs.

Skäl för förslaget: Den personuppgiftsansvarige skall, enligt 48 § personuppgiftslagen (1998:204), ersätta den registrerade för skada och kränkning av den personliga integriteten som en behandling av personuppgifter i strid med lagen har orsakat. Ersättningsskyldigheten kan, som framgår av bestämmelsen, jämkas, om den personuppgiftsansvarige visar att felet inte berodde på honom eller henne. Den personuppgiftsansvarige är således ersättningsskyldig gentemot den registrerade så snart en behandling av personuppgifter har skett i strid med någon bestämmelse i lagen, såsom t.ex. någon av bestämmelserna om grundläggande krav på personuppgiftsbehandlingen. Det krävs inte att den personuppgiftsansvarige har haft uppsåt att handla i strid med lagen eller varit oaktsam. Ersättningsskyldighet föreligger alltså även när den personuppgiftsansvarige bevisligen är oskyldig till felet (prop. 1997/98:44 s. 107). Bakgrunden till denna stränga reglering är att bestämmelsen om skadestånd, precis som enskildas rättigheter i övrigt enligt lagen – rätt till information och rättelse

m.m. – har till syfte att skydda människor mot kränkning av den personliga integriteten genom behandling av personuppgifter.

Även de lagar som föreslås här syftar till att skydda människors personliga integritet. Motsvarande rätt till skadestånd för den enskilde bör därför finnas för skada och kränkning som uppstår när Försvarsmakten respektive Försvarets radioanstalt behandlar uppgifter i strid med bestämmelserna i de lagförslag som föreslås i denna promemoria.

Göteborgs universitet har i sitt remissvar föreslagit att preskriptionstiden för rätten till skadestånd skall räknas från den tidpunkt då den skadelidande får kännedom om den skadebringande handlingen och inte från tidpunkten då den skadebringande handlingen företogs. Eftersom den skadelidande kanske får kännedom om den skadebringande handlingen först lång tid efter det att handlingen vidtogs anser universitetet att skadeståndsrätten i annat fall riskerar att bli utan verkan.

Preskriptionstiden i fråga om fordringar i allmänhet är som huvudregel 10 år från fordringens tillkomst, 2 § preskriptionslagen (1981:130). Preskriptionstiden avseende fordringar på skadestånd räknas normalt från den dag den skadegörande handlingen begås. Den fråga som Göteborgs universitet har väckt rör de grundläggande principerna om beräkning av preskriptionstid för fordringar på skadestånd. Frågan bör lösas på ett gemensamt sätt, åtminstone för de myndigheter som bedriver underrättelseverksamhet. Några överväganden eller förslag som avviker från vad som gäller idag i denna del kan inte göras inom ramen för denna promemoria.

8.14 Säkerheten vid behandling

<p>Förslag: Ett personuppgiftsbiträde och den eller de personer som arbetar under bitrådets eller Försvarsmaktens respektive Försvarets radioanstalts ledning får behandla personuppgifter bara i enlighet med instruktioner från Försvarsmakten respektive Försvarets radioanstalt.</p>

Det skall finnas ett skriftligt avtal om personuppgiftsbitrådets behandling av personuppgifter för Försvarmaktens respektive Försvarets radioanstalts räkning. I det avtalet skall det särskilt föreskrivas att personuppgiftsbitrådet får behandla personuppgifterna bara i enlighet med instruktioner från myndigheten och att personuppgiftsbitrådet är skyldigt att vidta vissa säkerhetsåtgärder.

Försvarmakten respektive Försvarets radioanstalt skall vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna skall åstadkomma en säkerhetsnivå som är lämplig med beaktande av bl.a. de tekniska möjligheter som finns och hur pass känsliga de behandlade personuppgifterna är.

När Försvarmakten respektive Försvarets radioanstalt anlitar ett personuppgiftsbiträde, skall myndigheten förvissa sig om att personuppgiftsbitrådet kan genomföra de säkerhetsåtgärder som måste vidtas och se till att personuppgiftsbitrådet verkligen vidtar åtgärderna.

Tillgången till personuppgifter skall alltid begränsas till vad personen behöver för att kunna fullgöra sina arbetsuppgifter.

Utredningens förslag överensstämmer i princip med promemorians förslag. Utredningens förslag saknar dock ett förslag till reglering av tillgången till personuppgifterna.

Remissinstanserna tillstyrker eller har inte något att invända.

Skäl för förslaget: I 30–32 §§ personuppgiftslagen (1998:204) finns regler om hur den personuppgiftsansvarige skall organisera arbetet med behandlingen av personuppgifter för att garantera säkerheten. Det rör sig om instruktioner till personalen samt tekniska och organisatoriska åtgärder.

Således föreskrivs i 30 § att ett personuppgiftsbiträde och den eller de personer som arbetar under bitrådets eller den personuppgiftsansvariges ledning får behandla personuppgifter bara i enlighet med instruktioner från den personuppgiftsansvarige. Där anges också att det skall finnas ett skriftligt avtal om personuppgiftsbitrådets behandling av personuppgifter för den per-

sonuppgiftsansvariges räkning. I avtalet skall det särskilt föreskrivas att biträdet får behandla personuppgifter endast i enlighet med den personuppgiftsansvariges instruktioner och att biträdet är skyldigt att vidta de säkerhetsåtgärder som avses i 31 § första stycket, se nedan. I fråga om sekretess och tystnadsplikt i det allmännas verksamhet tillämpas istället bestämmelserna i sekretesslagen (1980:100).

Av 31 § personuppgiftslagen följer att den personuppgiftsansvarige skall vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna skall åstadkomma en säkerhetsnivå som är lämplig med beaktande av de tekniska möjligheter som finns, vad det skulle kosta att genomföra åtgärderna, de särskilda risker som finns med behandlingen av personuppgifterna och hur pass känsliga de behandlade personuppgifterna är. När den personuppgiftsansvarige anlitar ett personuppgiftsbiträde skall den personuppgiftsansvarige förvissa sig om att biträdet kan genomföra de säkerhetsåtgärder som måste vidtas och se till att biträdet verkligen vidtar åtgärderna.

Det kan ifrågasättas vilken funktion det fyller att för Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst samt Försvarets radioanstalts underrättelse- och utvecklingsverksamhet föreslå bestämmelser som motsvarar de i 30 och 31 §§ personuppgiftslagen. Den tekniska säkerheten vad gäller intrångsskydd, behörighetsnivåer för tillgång till behandlade uppgifter samt spridningsbegränsningar m.m. (se avsnitt 3 och 4) är av naturen av största betydelse för den militära underrättelse- och säkerhetstjänsten och Försvarets radioanstalt, redan av andra skäl än personuppgiftslagens bestämmelser. Så har t.ex. Försvarets radioanstalts utvecklade säkerhetstänkande och högt kvalificerade tekniska kompetens medfört att myndigheten getts i uppdrag att tillhandahålla teknikkompetens inom den offentliga sektorn (se 3 a § förordning [1994:714] med instruktion för Försvarets radioanstalt och prop. 2001/02:158 s. 109 f). För att understryka att säkerheten vid behandling är viktig inte bara med hänsyn till verksamheten som sådan utan också för skyddet av

den personliga integriteten bör lagförslagen ändå innehålla bestämmelser om personer som behandlar personuppgifter och säkerhetsåtgärder.

Därutöver bör det i en särskild bestämmelse anges att tillgången till personuppgifter alltid skall begränsas till vad personen behöver för att kunna fullgöra sina arbetsuppgifter. En sådan bestämmelse är angelägen med hänsyn till skyddet av den personliga integriteten.

Tillsynsmyndigheten får, enligt 32 § och 45 § andra stycket personuppgiftslagen, i enskilda fall besluta om vilka säkerhetsåtgärder den personuppgiftsansvarige skall vidta samt förena beslutet med vite. Som utredningen framför är det inte lämpligt att tillsynsmyndigheten skall ha befogenhet att tala om för Försvarsmakten och Försvarets radioanstalt vilka säkerhetsåtgärder myndigheten skall vidta i detta sammanhang. Lagförslagen innehåller därför inte någon bestämmelse som motsvarar den i 32 § och 45 § andra stycket personuppgiftslagen.

8.15 Personuppgiftsombud m.m.

Förslag: Försvarsmakten respektive Försvarets radioanstalt skall utse ett eller flera personuppgiftsombud och anmäla dessa till den tillsynsmyndighet som avses i avsnitt 8.16. Även ett entledigande av ett personuppgiftsombud skall anmälas till tillsynsmyndigheten.

Personuppgiftsombudet skall ha till uppgift att självständigt se till att Försvarsmakten respektive Försvarets radioanstalt behandlar personuppgifter på ett lagligt och korrekt sätt och i enlighet med god sed samt påpeka eventuella brister för myndigheten. Om personuppgiftsombudet har anledning att misstänka att myndigheten bryter mot de bestämmelser som gäller för behandlingen och vidtas inte rättelse så snart det kan ske efter påpekande, skall personuppgiftsombudet anmäla förhållandet till tillsynsmyndigheten.

Personuppgiftsombudet skall föra en förteckning över de handlingar som Försvarsmakten respektive Försvarets radioan-

stalt genomför och som är helt eller delvis automatiserade. Personuppgiftsombudet skall hjälpa registrerade att få rättelse när det finns anledning att misstänka att behandlade personuppgifter är felaktiga eller ofullständiga.

Utredningens förslag överensstämmer med promemorians.

Remissinstanserna tillstyrker eller har inte något att invända mot förslagen.

Skäl för förslaget:

Anmälningsskyldighet för helt eller delvis automatiserade behandlingar

Behandling av personuppgifter som är helt eller delvis automatiserad omfattas, enligt 36 § första stycket personuppgiftslagen (1998:204), av anmälningsskyldighet till tillsynsmyndigheten. Bestämmelsen har sin bakgrund i dataskyddsdirektivet. Regeringen uttalade i samband med införandet av personuppgiftslagen att det var viktigt att fullt ut utnyttja de möjligheter till undantag från anmälningsskyldigheten som direktivet medger och på så sätt begränsa anmälningsskyldigheten till ett minimum (se prop. 1997/98:44 s. 98). Anmälningsskyldigheten har mot denna bakgrund på olika sätt begränsats. I 3 § 3 personuppgiftsförordningen (1998:1191) har t.ex. angetts att anmälningsskyldigheten inte gäller för behandlingar av personuppgifter som regleras genom särskilda föreskrifter i lag eller förordning. Vidare har i 37 § personuppgiftslagen föreskrivits att om den personuppgiftsansvarige till tillsynsmyndigheten anmält att ett personuppgiftsombud utsetts och vem det är, så behöver inte sådan anmälan till tillsynsmyndigheten göras.

Behandlingen av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst samt Försvarets radioanstalts underrättelse- och utvecklingsverksamhet kommer att regleras av de lagar som läggs fram här jämte förordningar som ansluter till dessa. Det finns därför inte skäl att ställa krav på anmälningsskyldighet för behandlingar som är helt eller delvis automatiserade och som utförs med stöd av dessa författ-

ningar. Bestämmelser motsvarande de i 36 § första och tredje stycket och 37 § personuppgiftslagen skall därför inte gälla.

Personuppgiftsombud

Enligt 36 § andra stycket personuppgiftslagen skall den personuppgiftsansvarige om han eller hon utser ett personuppgiftsombud anmäla detta till tillsynsmyndigheten. Även ett entledigande av ett personuppgiftsombud skall anmälas till tillsynsmyndigheten, 36 § andra stycket personuppgiftslagen.

Personuppgiftsombudet har att självständigt se till att den personuppgiftsansvarige behandlar personuppgifter på ett lagligt och korrekt sätt och i enlighet med god sed samt att påpeka eventuella brister för denne. Har personuppgiftsombudet anledning att misstänka att den personuppgiftsansvarige bryter mot de bestämmelser som gäller för behandlingen av personuppgifter och vidtas inte rättelse så snart det kan ske efter påpekande, skall personuppgiftsombudet anmäla förhållandet till tillsynsmyndigheten. Personuppgiftsombudet skall även i övrigt samråda med tillsynsmyndigheten vid tveksamhet om hur de bestämmelser som gäller för behandlingen av personuppgifter skall tillämpas, 38 § personuppgiftslagen.

Vidare skall personuppgiftsombudet föra en förteckning över de behandlingar som den personuppgiftsansvarige genomför och som skulle ha omfattats av anmälningsskyldighet om ombudet inte hade funnits, 39 § personuppgiftslagen. Personuppgiftsombudet skall hjälpa registrerade att få rättelse när det finns anledning att misstänka att behandlade personuppgifter är felaktiga eller ofullständiga, 40 § personuppgiftslagen.

I denna promemoria uppställs ett krav på myndigheterna att ha ett personuppgiftsombud och att anmäla dessa till den tillsynsmyndighet som föreslås i avsnitt 8.16. Även ett entledigande av ett personuppgiftsombud skall anmälas till tillsynsmyndigheten. Såväl Försvarmakten som Försvarets radioanstalt har redan idag utsett personuppgiftsombud som på ett oberoende sätt har att säkerställa den interna tillämpningen av bestämmelser om

personuppgiftsbehandling. Personuppgiftsombudens uppgifter skall även i fortsättningen överensstämma med de som finns i 38–40 §§ personuppgiftslagen.

Särskilt integritetskänsliga behandlingar

Regeringen får enligt 41 § personuppgiftslagen meddela föreskrifter om att sådana behandlingar av personuppgifter som innebär särskilda risker för otillbörligt intrång i den personliga integriteten skall för förhandskontroll anmälas till tillsynsmyndigheten tre veckor i förväg. Bestämmelsen har sin bakgrund i dataskyddsdirektivet.

Någon sådan föreskrift som avses i 41 § personuppgiftslagen har idag inte meddelats vad gäller personuppgiftsbehandling i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst samt i Försvarets radioanstalts underrättelse- och utvecklingsverksamhet. Försvarsunderrättelseverksamheten bedrivs med inriktning på utländska förhållanden och till stöd för svensk utrikes-, säkerhets- och försvarspolitik. Därutöver bedriver Försvarets radioanstalt viss annan underrättelseverksamhet. Regeringen bestämmer inriktningen av dessa underrättelseverksamheter, se avsnitt 8.5. Med hänsyn till verksamheternas art och förslaget i avsnitt 8.16 om en särskild granskning till skydd för den personliga integriteten lämnas inte här något förslag på en bestämmelse motsvarande den i 41 § personuppgiftslagen.

Upplysningar till allmänheten om behandlingar som inte anmälts

Bestämmelserna i 42 § personuppgiftslagen ålägger den personuppgiftsansvarige en generell skyldighet att till var och en som efterfrågar det lämna information om behandlingar av personuppgifter som inte har anmälts till tillsynsmyndigheten. Upplysningarna skall omfatta det som en anmälan om helt eller delvis automatiserade behandlingar annars skulle ha omfattat. Upplysning behöver emellertid inte lämnas om uppgifter som omfattas

av sekretess. I Datainspektionens föreskrifter (DIFS 1998:2) regleras vilka uppgifter en sådan anmälan skall innehålla. De flesta av dessa uppgifter är sådana som framgår av den föreslagna författningstexten, t.ex. vem den personuppgiftsansvarige är och vilket ändamål behandlingen har. Övriga är sådana som i försvarsunderrättelseverksamhet och säkerhetstjänst typiskt sett omfattas av sekretess, t.ex. upplysning om överföring till tredje land och vilka säkerhetsåtgärder som vidtagits. Med hänsyn härtill skulle en hänvisning till 42 § personuppgiftslagen inte vara till någon nytta för enskilda. Någon bestämmelse motsvarande den i 42 § personuppgiftslagen föreslås därför inte.

8.16 Tillsyn och särskild granskning till skydd för den personliga integriteten

Förslag: Den myndighet som regeringen bestämmer skall utöva tillsyn över att den behandling av personuppgifter som sker inom Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst samt i Försvarets radioanstalts underrättelse- och utvecklingsverksamhet sker i enlighet med de föreslagna lagarna. I förordningar som skall anknyta till lagarna skall anges att Datainspektionen är sådan tillsynsmyndighet.

Därutöver skall Försvarets underrättelsenämnd till skydd för den personliga integriteten särskilt granska de behandlingar av personuppgifter som sker. Detta skall komma till uttryck i nämndens instruktion.

Utredningens förslag överensstämmer i princip med promemorians. Utredningen föreslog därutöver att Försvarets underrättelsenämnds ansvarsområde skulle utökas till att omfatta den militära säkerhetstjänsten i dess helhet.

Remissinstanserna: De flesta remissinstanser, såsom bl.a. *Försvarsmakten* och *Försvarets radioanstalt*, tillstyrker eller har inget att invända mot utredningens förslag. *Rikspolisstyrelsen* och *Säkerhetspolisen* tillstyrker att Försvarets underrättelsenämnd ges i uppdrag att granska behandlingen av personuppgifter hos För-

svarsmakten och Försvarets radioanstalt på liknande sätt som Registernämnden granskar Säkerhetspolisens behandling av personuppgifter. *Registernämnden*, som också tillstyrker förslaget, menar att det måste vara till fördel för en granskning att den utförs av ett organ, som har till uppgift att följa underrättelseverksamheten i dess helhet inom försvaret och som därmed kan göra mera principiella överväganden om tillåtligheten av olika förfaranden, än av ett nyinrättat kontrollorgan med en begränsad uppgift. *Datainspektionen* saknar en närmare analys om varför Försvarets underrättelsenämnd inte i likhet med Registernämnden skall få fatta beslut om utlämnande i enskilda fall. *Försvarets underrättelsenämnd*, som inte har någon erinran mot de förslag som rör myndigheten, understryker att de förslag som rör nämnden inte får leda till att nämnden blir involverad i någon löpande ärendehantering. *Kustbevakningen* delar uppfattningen att det bör finnas ett särskilt granskningsorgan till skydd för den personliga integriteten. Kustbevakningen är emellertid inte övertygad om att denna funktion bäst utövas på föreslaget sätt om syftet är att stärka enskildas integritetsskydd. Kustbevakningen ifrågasätter hur nämnden skall verka och på bästa sätt ta till vara enskildas intressen utan att själv bli inblandad i ärendehantering- en då någon enskild begär att få ut handlingar. *Göteborgs universitet* föreslår att ett oberoende kontrollorgan införs med samma funktion som den som utredningen föreslår, men avstyrker utredningens förslag att Försvarets underrättelsenämnd får denna roll. Universitetet föreslår att det införs krav på att kontrollorganet, till riksdagen, avlämnar en årlig redovisning och utvärdering av Försvarsmaktens och Försvarets radioanstalts registrering och behandling av personuppgifter vad avser omfattning och innehåll i förhållande till i lagarna angivna ändamål.

Skäl för förslaget:

Tillsyn

Varje medlemsstat skall enligt artikel 28 dataskyddsdirektivet utse en eller flera myndigheter som har till uppgift att inom dess territorium övervaka tillämpningen av de bestämmelser som

medlemsstaterna antar till följd av direktivet. I direktivet anges att dessa myndigheter skall fullständigt oberoende utöva de uppgifter som åläggs dem.

Datainspektionen är en sådan tillsynsmyndighet som avses i direktivet, 2 § förordning (1998:1192) med instruktion för Datainspektionen och 2 § personuppgiftsförordningen (1998:1191). Datainspektionen utövar redan idag tillsyn över Försvarsmaktens och Försvarets radioanstalts personuppgiftsbehandling och föreslås här göra det också i fortsättningen.

I denna promemoria föreslås således att det i lagförslagen skall anges att den tillsynsmyndighet som regeringen bestämmer skall utöva tillsyn över Försvarsmaktens och Försvarets radioanstalts behandling av personuppgifter. Av de förordningar som skall ansluta till lagarna skall framgå att Datainspektionen är sådan tillsynsmyndighet.

Särskild granskning

De bestämmelser som föreslås i avsnitt 8.11 om enskildas rätt till information hör till de viktigaste medlen för att personuppgifter inte skall behandlas på ett sätt som kan medföra att enskildas personliga integritet kränks. Sekretess och tystnadsplikt föreslås emellertid gå före skyldigheten för Försvarsmakten och Försvarets radioanstalt att lämna information till den enskilde (se nämnda avsnitt). Den sekretess som gäller för uppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst och Försvarets radioanstalts underrättelse- och utvecklingsverksamhet innebär att information sällan kommer att lämnas av myndigheterna. Utan kunskap om vilka uppgifter som behandlas av Försvarsmakten och Försvarets radioanstalt kommer den enskilde inte att kunna utnyttja möjligheten att begära rättelse eller i övrigt kontrollera att uppgifter om honom eller henne behandlas korrekt och i enlighet med vad som är särskilt föreskrivet. För att åstadkomma ett bättre skydd för de enskildas personliga integritet är det nödvändigt att värna denna på något annat sätt. Den aktuella behandlingen av personuppgifter hos

Försvarmakten och Försvarets radioanstalt bör därför genom statsmakternas försorg underkastas en särskild granskning till skydd för den personliga integriteten.

När man överväger val av granskningsorgan är hänsynen till sekretessen inom underrättelseverksamheten och den militära säkerhetstjänsten av stor betydelse. Ett alternativ till granskningsorgan är då Försvarets underrättelsenämnd. Nämnden inrättades 1976, efter förslag av Underrättelseutredningen (SOU 1976:19). Utredningen, som konstaterade att en djup sekretess är nödvändig kring stora delar av det militära underrättelseväsendet och att enskilda har små möjligheter att informera sig om denna, ansåg att det därför var betydelsefullt att begränsningarna i den enskilda insynen uppvägdes av en effektivt verkande kontroll genom statsmakternas försorg (a. a. s. 129).

Försvarets underrättelsenämnd har, enligt sin instruktion, till uppgift att följa underrättelsetjänsten inom de myndigheter som bedriver försvarsunderrättelseverksamhet, såsom t.ex. Försvarmakten och Försvarets radioanstalt. Nämnden skall särskilt följa bl.a. hur lagen (2000:130) om försvarsunderrättelseverksamhet och den därtill hörande förordningen tillämpas, granska att försvarsunderrättelseverksamheten bedrivs i enlighet med den inriktning som är bestämd, ägna uppmärksamhet åt de enheter inom Försvarmakten och Försvarets radioanstalt som inhämtar underrättelser med särskilda metoder samt granska hur de register som behövs för försvarsunderrättelseverksamheten läggs upp och förs. Nämnden skall lämna Försvarmakten och Försvarets radioanstalt de synpunkter och de förslag till åtgärder som föranleds av granskningen. Om det behövs skall nämnden också lämna förslag om åtgärder till regeringen. Nämnden skall senast den 1 mars varje år till regeringen lämna en rapport över föregående års granskningsverksamhet. Nämnden består av sex ledamöter, varav en är ordförande, som utses för en bestämd tid. Vid nämnden finns en sekreterare. Samtliga utses av regeringen, 1-5 §§ förordning (1988:552) med instruktion för Försvarets underrättelsenämnd. Av 5-6 §§ förordningen (2000:131) om försvarsunderrättelseverksamhet framgår att Försvarmakten och Försva-

rets radioanstalt ålagts att informera nämnden i frågor som rör försvarsunderrättelseverksamhet.

I Ds 2005:30 föreslås att nämnden, förutom att kontrollera försvarsunderrättelseverksamheten, skall kontrollera även Försvarets radioanstalts inhämtning enligt den föreslagna lagen om signalspaning. Nämndens organisation föreslås bli förstärkt med ytterligare en ledamot, som liksom en av de förutvarande ledamöterna skall vara eller ha varit ordinarie domare. Vidare skall ett kansli under ledning av en kanslichef inrättas. I kansliet bör finnas god kunskap om underrättelsearbete och juridisk kompetens. Det föreslås att kanslichefen, liksom ledamöterna, skall utses av regeringen. Förslagen möjliggör enligt promemorian att nämnden kan utföra en mer ingående kontroll av verksamheten och att verksamheten kan följas löpande (se vidare avsnitt 6).

Ett alternativ till granskningsorgan är ett nyinrättat organ med begränsad tillsynsuppgift. Med hänsyn till verksamheternas särskilda art och deras betydelse för rikets säkerhet kan dock lämpligheten av att inrätta ett sådant granskningsorgan med begränsad uppgift vid sidan av Försvarets underrättelsenämnd ifrågasättas. Försvarets underrättelsenämnd har redan idag till uppgift att granska hur de register som behövs i försvarsunderrättelseverksamheten läggs upp och förs. Nämnden har också vana att iaktta den sekretess som gäller för uppgifter i underrättelsetjänsten och har kunskaper om såväl försvarsunderrättelseverksamhet i dess helhet som signalspaningsverksamhet. Förslaget om en förstärkning av nämndens organisation innebär dessutom att nämnden kommer ha bättre förutsättningar att utöva tillsyn över Försvarsmakten och Försvarets radioanstalt än tidigare. Försvarets underrättelsenämnd får mot denna bakgrund anses bäst lämpad att utföra särskild granskning av behandlingen av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst och Försvarets radioanstalts underrättelse- och utvecklingsverksamhet. Här föreslås således – vilket också tillstyrkts av de flesta remissinstanser, däribland Datainspektionen, Försvarets underrättelsenämnd, Försvarsmakten och Försvarets radioanstalt – att Försvarets underrättelsenämnds upp-

drag skall utökas till att omfatta granskning av behandlingen av personuppgifter enligt de lagförslag som lämnas här. Detta skall komma till uttryck i nämndens instruktion.

Försvarets underrättelsenämnds särskilda granskningsuppgift inskränker inte Datainspektionens övergripande tillsynsansvar. Datainspektionen har således alltjämt huvudansvaret för tillsynen över behandlingen av personuppgifter hos Försvarmakten och Försvarets radioanstalt och föreslås att för denna uppgift få de befogenheter som anges i avsnitt 8.17. Försvarets underrättelsenämnds särskilda granskning skall utgöra en kompensation för att enskilda, på grund av den sekretess som gäller, inte i tillräcklig utsträckning kan utnyttja den möjlighet till skydd för den personliga integriteten som föreslagna bestämmelser om information och rättelse m.m. innebär. Nämndens granskning är således en extra integritetsskyddskontroll som, utöver Datainspektionens tillsyn, syftar till att skydda de registrerade mot att deras personliga integritet kränks genom behandling av personuppgifter. Nämndens granskning kan jämföras med Registernämndens granskning av Säkerhetspolisens behandling av personuppgifter enligt polisdatalagen (1988:622). Registernämndens granskning förtar inte Datainspektionens tillsynsansvar över behandlingar av personuppgifter enligt polisdatalagen.

Datainspektionen och Kustbevakningen ifrågasätter hur nämnden skall verka och på bästa sätt ta till vara enskildas intressen utan att själv bli inblandad i ärendehantering då någon enskild begär att få ut handlingar. *Försvarets underrättelsenämnd* anser å andra sidan att de förslag som rör nämnden inte får leda till att nämnden blir involverad i någon löpande ärendehantering.

En av Registernämndens uppgifter är att se till att personer som skall anlitas av t.ex. staten där känslig verksamhet förekommer inte utgör en risk för Sveriges säkerhet. I 1 § förordning (1996:730) med instruktion för Registernämnden föreskrivs således att Registernämnden i ärenden om registerkontroll enligt säkerhetsskyddslagen (1996:730) prövar frågor om utlämnande av uppgifter från vissa av polisens register bl.a. sådana register som omfattas av polisdatalagen. Innan en uppgift som har kom-

mit fram vid registerkontroll får lämnas ut av nämnden för säkerhetsprövning skall den som uppgiften avser ges tillfälle att yttra sig över den, 25 § säkerhetsskyddslagen. Undantag gäller för uppgift som omfattas av sekretess i förhållande till den enskilde, samma bestämmelse. Den som önskar att ta del av uppgifter i polisens verksamhet måste vända sig till polisen och inte Registernämnden. Registernämnden handlägger således inte begäran från enskilda om utlämnande av sådana uppgifter.

Inte heller Försvarets underrättelsenämnd skall handlägga begäran från enskilda om utlämnande av uppgifter. En begäran från enskild om utlämnande av allmän handling skall på samma sätt som i dag prövas av Försvarmakten respektive Försvarets radioanstalt och avslagsbeslut eller beslut om utlämnande med förbehåll får överklagas av sökanden, 15 kap. 7 § sekretesslagen (1980:100). Det ankommer på nämnden att, i enlighet med vad som annars gäller för självständiga tillsynsorgan, bestämma de närmare formerna för hur nämndens särskilda granskning skall utformas.

Utredningen föreslår att Försvarets underrättelsenämnd skall granska den militära säkerhetstjänsten i dess helhet. Nämnden har idag inte något uppdrag att kontrollera tjänsten som sådan. Som utredningen angett, har dock nämnden på uppdrag av regeringen 1998 granskat den militära säkerhetstjänstens arkiv för åren 1931-1981. Utredningen anser att Försvarets underrättelsenämnd bör, för att kunna granska behandlingen av personuppgifter i den militära säkerhetstjänsten, kontrollera tjänsten i dess helhet. En granskning av personuppgiftsbehandling förutsätter emellertid inte att granskningsorganet kontrollerar även verksamheten i dess helhet. Datainspektionens och Registernämndens granskning är två exempel på detta. Utredningen har endast mycket kort beskrivit sina överväganden när det gäller att utöka Försvarets underrättelsenämnds tillsynsmandat i denna del. Överväganden och underlag om bl.a. tillsynens omfattning, befogenheter, konsekvenser för organisationen samt ekonomiska konsekvenser saknas. I denna promemoria finns därför inte underlag för att gå vidare med utredningens förslag i denna del.

8.17 Tillsynsmyndighetens och det särskilda granskningsorganets befogenheter

Förslag: Tillsynsmyndigheten skall ha rätt att för sin tillsyn på begäran få

1. tillgång till de personuppgifter som behandlas,
2. upplysningar om och dokumentation av behandlingen av personuppgifter och säkerheten vid denna, och
3. tillträde till sådana lokaler som har anknytning till behandlingen av personuppgifter.

Om tillsynsmyndigheten konstaterar att personuppgifter behandlas eller kan komma att behandlas på ett olagligt sätt, skall myndigheten genom påpekanden eller liknande förfaranden försöka åstadkomma rättelse.

Tillsynsmyndigheten får hos länsrätten i Stockholms län ansöka om att sådana personuppgifter som har behandlats på ett olagligt sätt skall utplånas. Beslut om utplånande får inte meddelas om det är oskäligt.

Det särskilda granskningsorganet skall ha rätt att få tillgång till de personuppgifter som behandlas.

Utredningens förslag överensstämmer i huvudsak med promemorians. Utredningens förslag saknar möjlighet för tillsynsmyndigheten att genom påpekanden eller liknande försöka åstadkomma rättelse.

Remissinstanserna: De flesta remissinstanser tillstyrker eller har inget att erinra mot utredningens förslag. *Hovrätten för Övre Norrland* ställer sig dock tveksam till utredningens överväganden och konstaterar att förslaget medför att tillsynsmyndigheten utan begränsningar har tillgång till kvalificerat hemliga personuppgifter som hanteras i de aktuella verksamheterna samt tillträde till lokaler med anknytning till sådan behandling. Hovrätten ifrågasätter den av utredningen valda lösningen med tanke på verksamheternas särskilda art och deras betydelse för rikets säkerhet.

Skäl för förslaget: För att tillsynsmyndigheten på ett så effektivt sätt som möjligt skall kunna utöva tillsyn över den behand-

ling av personuppgifter som förekommer har myndigheten enligt personuppgiftslagen rätt att på begäran få tillgång till de personuppgifter som behandlas, upplysningar om och dokumentation av behandlingen av personuppgifter och säkerheten vid denna samt tillträde till lokaler som har anknytning till behandlingen, 43 §. Om tillsynsmyndigheten konstaterar att personuppgifter behandlas eller kan komma att behandlas på ett olagligt sätt skall myndigheten genom påpekanden eller liknande förfaranden försöka åstadkomma rättelse, 45 § första stycket 1. Tillsynsmyndigheten kan också, beträffande personuppgifter som har behandlats olagligt, ansöka hos länsrätten om att dessa skall utplånas, 47 §. Beslut om utplånande får enligt paragrafen inte meddelas om det är oskäligt.

I denna promemoria föreslås att tillsynsmyndigheten för att kunna bedriva en effektiv kontroll skall ha motsvarande befogenheter vid sin tillsyn av personuppgiftsbehandlingen i Försvarsmakten försvarsunderrättelseverksamhet och militära säkerhetstjänst och Försvarets radioanstalts underrättelse- och utvecklingsverksamhet.

Bestämmelserna i 44 §, 45 § första stycket 2 och andra stycket samt 46 § personuppgiftslagen ger tillsynsmyndigheten möjlighet att vid vite förbjuda en personuppgiftsansvarig att behandla personuppgifter. Således kan tillsynsmyndigheten, om den inte efter begäran kan få tillräckligt underlag för att konstatera att behandlingen av personuppgifter är laglig, vid vite förbjuda den personuppgiftsansvarige att behandla personuppgifter på något annat sätt än genom att lagra dem, 44 §. Som framgått kan tillsynsmyndigheten också under vissa förutsättningar genom påpekanden eller liknande förfaranden försöka åstadkomma rättelse. Går det inte att få rättelse på något annat sätt eller är saken brådskande, får tillsynsmyndigheten vid vite förbjuda den personuppgiftsansvarige att fortsätta att behandla personuppgifterna på något annat sätt än genom att lagra dem, 45 § första stycket.

Utredningen, som funnit att vite inte bör användas som sanktionsmedel mellan statliga myndigheter, föreslår att bestämmel-

serna om vite inte skall var tillämpliga vid tillsyn av behandling av personuppgifter i de nu aktuella verksamheterna. Remissinstanserna har tillstyrkt eller inte haft någon invändning mot utredningens förslag. Frågor som uppkommer i samband med tillsynsmyndighetens granskning måste kunna lösas genom en dialog mellan tillsynsmyndigheten och den berörda myndigheten. Denna promemoria innehåller därför inte några förslag till bestämmelser om vite.

Försvarets underrättelsenämnd skall för fullgörandet av sin särskilda granskningsuppgift ha rätt att få tillgång till de personuppgifter som behandlas i Försvarets försvarsunderrättelseverksamhet och militära säkerhetstjänst och Försvarets radioanstalts underrättelse- och utvecklingsverksamhet (jfr. Registernämndens befogenheter enligt 11 § förordning [1996:730] med instruktion för Registernämnden). Detta skall komma till uttryck i Försvarets underrättelsenämnds instruktion.

Datainspektionen utövar redan i dag tillsyn över Försvarets radioanstalts behandling av personuppgifter och har därvid – i avsaknad av särskild reglering i förordning (2001:703) om viss behandling av personuppgifter inom Försvarets radioanstalt – de befogenheter som enligt personuppgiftslagen tillkommer tillsynsmyndigheten. Mot den bakgrunden föranleder inte de farhågor som *Hovrätten för Övre Norrland* uttryckt angående tillsynsmyndighetens tillgång till hemliga uppgifter och tillträde till de lokaler där verksamheten bedrivs någon annan bedömning än den nyss redovisade.

8.18 Straff

Förslag: Den som uppsåtligen eller av grov oaktsamhet lämnar osanna uppgifter i information till den om vilken personuppgifter behandlas eller till tillsynsmyndigheten straffas med böter eller fängelse i högst sex månader. Detsamma gäller den som i strid med bestämmelserna behandlar känsliga personuppgifter. Om brottet är grovt är straffet fängelse i högst två år. I ringa fall skall inte dömas till ansvar.

Utredningen föreslår att straffbestämmelsen i 49 § personuppgiftslagen (1998:204) i dess helhet skall gälla vid Försvarmaktens och Försvarets radioanstalts behandling av personuppgifter.

Remissinstanserna tillstyrker eller har inte något att invända. *Hovrätten för Övre Norrland* anmärker att vissa av de bestämmelser som straffbestämmelsen i 49 § personuppgiftslagen hänvisar till har undantagits från de föreslagna lagarnas tillämpningsområde. Hovrätten anser att en sådan lagstiftningsteknik inte kan anses tillämplig i fråga om straffbestämmelser. Hänvisningen i lagförslagen bör enligt hovrätten formuleras så att det tydligt framgår vilka av de förfaranden som anges i 49 § personuppgiftslagen som är straffbara.

Skäl för förslaget: Det är få olagliga förfaranden som gjorts straffbara i personuppgiftslagen. All behandling av personuppgifter i strid med lagen kan föra med sig skyldighet att till de drabbade betala skadestånd och kan dessutom ytterst föranleda ett vitesföreläggande av tillsynsmyndigheten. Dessa sanktioner för brott mot lagen ansågs i samband med lagens tillkomst som effektiva och i stort sett tillräckliga (prop. 1997/98:44 s. 108). I straffbestämmelsen i 49 § föreskrivs således att den döms till böter eller fängelse i högst sex månader som uppsåtligen eller av oaktsamhet

a) lämnar osann uppgift i information till den registrerade, i anmälan till tillsynsmyndigheten enligt 36 § eller till tillsynsmyndigheten när myndigheten begär information enligt 43 §,

b) behandlar personuppgifter i strid med bestämmelserna i 13–21 §§ om känsliga personuppgifter och uppgifter om lagöverträdelser m.m.,

c) för över personuppgifter till tredje land i strid med 33–35 §§, eller

d) låter bli att göra anmälan om behandling av personuppgifter som är helt eller delvis automatiserad enligt 36 § första stycket eller enligt föreskrifter om förhandskontroll av särskilt integritetskänsliga behandlingar meddelade med stöd av 41 §.

Om brottet är grovt döms till fängelse i två år. I ringa fall döms inte till ansvar. Den som överträtt ett vitesföreläggande döms, enligt bestämmelsen, inte till ansvar för en gärning som omfattas av vitesföreläggandet.

I Personuppgiftslagsutredningens betänkande föreslås att endast uppsåtliga och grovt oaktsamma förfaranden skall vara straffbara (SOU 2004:6 s. 201).

Bestämmelser om straff vid visst förfarande med personuppgifter fyller en viktig funktion för att markera allvaret i överträdelser av regler till skydd för enskildas integritet. Straffbestämmelser motsvarande 49 § personuppgiftslagen bör därför intas i de föreslagna lagarna. Som *Hovrätten för Nedre Norrland* anmärkt har emellertid inte alla straffbelagda förfaranden enligt 49 § personuppgiftslagen någon motsvarighet i de föreslagna lagarna.

Lagarnas reglering av förutsättningarna för överföring av personuppgifter till andra länder beskrivs i avsnitt 8.10. Där framgår att bestämmelserna har en annan utformning än motsvarande bestämmelser i personuppgiftslagen. De senare anger som huvudregel ett förbud mot överföring av sådana uppgifter, vilket motiveras med att förfarandet innebär att personuppgifterna i praktiken försvinner inom räckhåll för svenska skyddsåtgärder (prop. 1997/98:44 s. 108 f). I de föreslagna lagarna medges i stället sådan överföring och anges under vilka förutsättningar den får äga rum (se vidare avsnitt 8.10). Bestämmelserna syftar till att uppfylla dataskyddskonventionens krav på nationell lagstiftning när det gäller överföring av personuppgifter till andra länder. Eftersom lagarna följaktligen inte innehåller något förbud mot överföring av personuppgifter utan anger att sådan överföring under vissa förutsättningar är tillåten, skall någon motsvarighet till det straffbelagda förfarandet i 49 § första stycket c personuppgiftslagen inte införas.

Enligt vad som framgår av avsnitt 8.15 föreskrivs i fråga om behandling av personuppgifter med stöd av de föreslagna författningarna inte någon anmälningsskyldighet enligt 36 § eller enligt föreskrift meddelad med stöd av 41 § personuppgiftslagen.

Till skillnad mot vad som gäller enligt 49 § första stycket i personuppgiftslagen skall följaktligen inte heller bland straffbara förfaranden anges underlåtenhet att göra sådan anmälan.

I avsnitt 8.17 konstateras att bestämmelser om möjlighet för tillsynsmyndigheten att vid vite förbjuda viss behandling av personuppgifter inte skall införas i lagarna. En bestämmelse motsvarande 49 § tredje stycket i personuppgiftslagen blir därmed överflödig.

I fråga om tillämplig straffskala och begränsningen av ansvar till fall som inte är ringa följer förslagen personuppgiftslagens reglering. I enlighet med Personuppgiftslagsutredningens ställningstagande föreslås att ansvar endast skall komma i fråga vid uppsåt och grov oaktsamhet. För en enskild vars integritet kränkts torde straffbestämmelserna vara sekundära i förhållande till möjligheten att erhålla skadestånd, vilket kan utgå även vid oaktsamhet. En begränsning av det straffbara området till fall av uppsåt och grov oaktsamhet får anses tillräckligt för att komma åt de särskilt klandervärda förfaranden som bör träffas av straffbestämmelserna.

8.19 Överklagande

Förslag: Försvarsmaktens respektive Försvarets radioanstalts beslut om information som skall lämnas och om rättelse får överklagas hos allmän förvaltningsdomstol. Andra beslut enligt denna lag får inte överklagas.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Utredningens förslag överensstämmer med promemorians.

Remissinstanserna tillstyrker eller har inte något att invända. *Länsrätten i Uppsala län* befarar att de föreslagna bestämmelserna kan innebära vissa tillämpningssvårigheter när Försvarsmakten respektive Försvarets radioanstalt, med hänvisning till sekretess, vägrar att lämna ut information som annars skulle lämnas enligt bestämmelserna om information till den registrerade. Det är enligt länsrätten oklart vilken domstol som skall pröva ett

överklagat beslut i ett sådant fall. Det kan enligt länsrätten förhålla sig så att det är kammarrätten som med stöd av sekretesslagen skall pröva om uppgifterna skall lämnas ut. Eftersom frågan i grunden gäller utlämnande av information enligt de föreslagna bestämmelserna är det enligt länsrättens mening dock möjligt att samma beslut även kan överklagas till länsrätten med stöd av de föreslagna överklagandebestämmelserna. Ett förtydligande av rättsläget i detta hänseende skulle enligt länsrättens mening vara befogat.

Skäl för förslaget: Enligt 51 § personuppgiftslagen får tillsynsmyndighetens beslut enligt lagen om annat än föreskrifter överklagas hos allmän förvaltningsdomstol. I bestämmelsen föreskrivs vidare att prövningstillstånd krävs vid överklagande till kammarrätten samt att tillsynsmyndigheten får bestämma att dess beslut skall gälla även om det överklagas. Personuppgiftslagen innehåller inte några andra bestämmelser om överklagande än de som återfinns i 51 §. Varken dataskyddskonventionen eller dataskyddsdirektivet kräver heller någon reglering av möjligheten att överklaga andra beslut än de som meddelats av tillsynsmyndigheten.

I de nu aktuella lagarna föreslås inte sådana befogenheter för tillsynsmyndigheten att bestämmelser om överklagande av tillsynsmyndighetens beslut är nödvändiga. Däremot kan Försvarsmakten respektive Försvarets radioanstalt med stöd av lagarna meddela beslut som berör enskilda. Så kan bli fallet med anledning av en enskilds begäran om information eller rättelse.

Beslut av en myndighet som direkt berör en enskild och som inte är av rent intern administrativ karaktär bör i allmänhet kunna överklagas. Den normala ordningen när en myndighet fattar beslut av förvaltningskaraktär är enligt 22 a § förvaltningslagen (1986:223) att beslutet kan överklagas hos allmän förvaltningsdomstol (länsrätt) och att det krävs prövningstillstånd för vidare överklagande till kammarrätten. Detta är också vad som generellt gäller enligt nyare författningar om behandling av personuppgifter i offentlig verksamhet, i vilka som regel anges att beslut om

information och rättelse kan överklagas till allmän förvaltningsdomstol.

I Personuppgiftslagsutredningens betänkande (SOU 2004:6 s. 205 ff.) föreslås en ny överklagandebestämmelse i personuppgiftslagen som avser myndighets beslut om information enligt 26 § personuppgiftslagen, om rättelse enligt 28 §, om information om automatiserade beslut enligt 29 § och om allmänna upplysningar om pågående behandlingar enligt 42 §. Besluten skall, såvitt här är av intresse, kunna överklagas till allmän förvaltningsdomstol (länsrätt) och prövningstillstånd skall krävas vid överklagande till kammarrätt.

I de lagar som föreslås regleras behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst samt i Försvarets radioanstalts underrättelse- och utvecklingsverksamhet bör införas en överklagandebestämmelse motsvarande vad som gäller enligt nyare registerförfattningar och som har föreslagits i fråga om personuppgiftslagen. Överklagande skall endast vara möjligt när det gäller sådana beslut enligt de föreslagna lagarna som direkt berör den enskilde, nämligen beslut att avslå en ansökan om information om pågående behandlingar samt beslut att avslå en begäran om rättelse.

Länsrätten i Uppsala län har påtalat att med den föreslagna ordningen kommer beslut med anledning av en enskilds begäran att ta del av en allmän handling respektive begäran om information om personuppgifter att överklagas till olika instanser, vilket kan medföra tillämpningsproblem.

Personuppgiftslagsutredningen har konstaterat att i de överklagandebestämmelser som intagits i nyare registerförfattningar har man inte anknutit till ordningen för överklagande av beslut att avslå en begäran om utfående av allmän handling, utan istället utgått från 22 a § förvaltningslagen. Personuppgiftslagsutredningen har inte funnit anledning att göra någon annan bedömning i fråga om sitt förslag till överklagandebestämmelse i personuppgiftslagen (SOU 2004:6 s. 220). Det bör eftersträvas att personuppgiftslagen och andra författningar som reglerar behandling av personuppgifter i offentlig verksamhet så långt möj-

ligt har enhetliga regleringar av sådana frågeställningar som är gemensamma, i synnerhet när det gäller processuella frågor. Den instansordning vid överklagande som gäller enligt nyare registerförfattningar bör därför inte frångås i fråga om behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst samt i Försvarets radioanstalts underrättelse- och utvecklingsverksamhet.

De tillämpningsproblem som Länsrätten i Uppsala län belyser får lösas genom att myndigheterna genom kontakter med den enskilde tydligt klargör om hans eller hennes begäran avser utfående av allmän handling eller information om personuppgifter som behandlas. Myndigheten har därefter att handlägga ärendet enligt tillämpligt regelverk och i händelse av överklagande överlämna detta till rätt instans. I de fall den enskildes ansökan avser såväl utfående av allmänna handlingar som information om personuppgifter får myndigheten handlägga ärendena separat och eventuella överklaganden prövas i olika instanser.

Andra beslut än de som särskilt anges skall inte kunna överklagas. Denna ordning överensstämmer med den reglering som återfinns i andra registerförfattningar och i Personuppgiftslagsutredningens förslag till överklagandebestämmelse. Ett beslut av myndigheten med anledning av en begäran om skadestånd kan följaktligen inte i sig överklagas. Däremot kan den enskilde alltid få frågan prövad genom att väcka talan vid allmän domstol. Någon särskild bestämmelse om detta är inte nödvändig.

8.20 Bevarande och gallring

Förslag: Personuppgifter som behandlas automatiserat skall gallras så snart uppgifterna inte längre behövs för de i lagarna angivna ändamålen. Regeringen får dock meddela föreskrifter eller beslut om att gallring skall ske senast vid viss tidpunkt.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om att personuppgifter utan hinder av gallringsbestämmelserna får bevaras för historiska, statistiska och vetenskapliga ändamål.

Utredningen föreslår inte någon särskild gallringsbestämmelse, vilket innebär att personuppgifter som behandlas i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst och i Försvarets radioanstalts underrättelse- och utvecklingsverksamhet skall bevaras och gallras enligt reglerna i personuppgiftslagen (1998:204) och arkivlagen (1990:782).

Remissinstanserna tillstyrker eller har inte något att erinra mot förslaget. *Försvarmakten* välkomnar utredningens förslag att inte införa några särskilda bestämmelser i fråga om bevarande och gallring av personuppgifter. Försvarmakten uppger att myndighetens inhämtning av personuppgifter för de föreslagna ändamålen många gånger är både tids- och kostnadskrävande och att uppgifterna ofta kan behöva sparas under mycket lång tid för att kunna ligga till grund för de bedömningar som behöver göras i försvarsunderrättelseverksamheten och den militära säkerhetstjänsten. Försvarmakten påpekar att bevarandet av denna typ av uppgifter har haft ett stort historiskt värde samt har bidragit till att ge en demokratisk insyn i underrättelse- och säkerhetstjänsten. *Kustbevakningen* anför att det bör vara ägnat att främja rättssäkerheten och integritetsskyddet att handlingar och uppgifter sparas under lång tid. Därigenom finns det enligt Kustbevakningen en åtminstone teoretisk garanti för att en enskild person i efterhand kan få klarlagt om han eller hon varit utsatt för en otillbörlig integritetskränkning. *Riksarkivet* välkomnar förslaget och konstaterar att förslaget innebär att allmänna handlingar i fortsättningen endast kommer gallras om det finns en föreskift utfärdad av Riksarkivet. Därmed ökas enligt Riksarkivet förutsättningarna för att handlingar kommer att behandlas enligt de regler och målsättningar som finns i tryckfrihetsförordningen och arkivlagen. Förslaget gör det möjligt för Riksarkivet att i samarbete med Försvarmakten och Försvarets radioanstalt ta itu med de stora bevarande- och gallringsfrågorna i databaserna. *Göteborgs universitet*, som stödjer utredningens förslag, anser att förslaget minskar risken för felaktig gallring och ökar rättssäkerheten samt möjligheten till framtida forskning. Universitetet

betonar särskilt vikten av att bevara källmaterial för framtida forskning.

Skäl för förslaget:

Personuppgiftslagen

Enligt 9 § första stycket i personuppgiftslagen (1998:204) får personuppgifter inte bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. Av tredje stycket samma lagrum framgår att personuppgifter får bevaras längre tid för historiska, statistiska eller vetenskapliga ändamål, dock inte under längre tid än vad som behövs för dessa ändamål.

Personuppgifter som utgör allmänna handlingar kan dock enligt 8 § andra stycket första meningen personuppgiftslagen arkiveras och bevaras utan hinder av lagens övriga bestämmelser, vilket då i stället sker under de förutsättningar som anges i arkivlagen (1990:782). I 3 § arkivlagen föreskrivs att myndigheters arkiv skall bevaras, hållas ordnade och vårdas så att de tillgodoser rätten att ta del av allmänna handlingar, behovet av information för rättsskipningen och förvaltningen samt forskningens behov. Allmänna handlingar får enligt 10 § samma lag endast gallras om återstående arkivmaterial kan tillgodose dessa ändamål, och det krävs särskilda föreskrifter eller beslut av arkivmyndighet för att gallring skall få ske.

Arkivlagens utgångspunkt är således att allmänna handlingar skall bevaras. I de särskilda registerförfattningar som reglerar behandling av personuppgifter i olika verksamheter är principen dock ofta den motsatta, nämligen att uppgifterna skall gallras senast efter viss tid om inte undantag har föreskrivits i registerförfattningen eller bestämmelse meddelad med stöd av denna. Principen att gallring skall ske motiveras i första hand av integritetsskäl (prop. 1989/90:72 s. 50 ff.). I 16 § förordningen (2001:703) om viss behandling av personuppgifter inom Försvarsmakten och Försvarets radioanstalt föreskrivs som huvudregel att personuppgifter som behandlats enligt förordningen skall gallras senast tio år efter den senast införda uppgiften om

den registrerade. Om det finns särskilda skäl får dock uppgifterna stå kvar under längre tid. Vidare föreskrivs att Riksarkivet efter samråd med myndigheterna får meddela föreskrifter om bevarande för historiska, statistiska eller vetenskapliga ändamål.

Behovet av gallringsbestämmelser

Med den i promemorian föreslagna lagstiftningstekniken blir inte personuppgiftslagens bestämmelser automatiskt tillämpliga för det fall att särskilda bestämmelser om bevarande och gallring saknas i lagarna. Utan uttrycklig reglering skulle därför endast arkivlagens huvudregel om bevarande gälla. Frågan är om detta i tillräcklig utsträckning skulle tillgodose kravet på integritetsskydd, i synnerhet med beaktande av att gallringsbestämmelser regelmässigt återfinns i särskilda registerförfattningar.

Behovet av gallringsbestämmelser måste avgöras efter en avvägning mellan å ena sidan intresset av skydd för den personliga integriteten och å andra sidan intresset av offentlighet och insyn i myndigheternas verksamhet. De personuppgifter som behandlas i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst samt Försvarets radioanstalts underrättelse- och utvecklingsverksamhet är typiskt sett av integritetskänslig natur. Å andra sidan kan offentlighetsprincipen och den minskade möjligheten till insyn i myndigheternas verksamhet för bl.a. forskning framhållas som skäl mot omfattande gallring i sådana till sin art så slutna verksamheter som de här aktuella.

En inledande frågeställning är om det finns anledning att göra olika överväganden beträffande behovet av gallringsbestämmelser beroende på hur lagringen av personuppgifterna sker. Ett traditionellt pappersbaserat lagringssystem utgör på grund av de begränsade möjligheterna att söka, bearbeta och sammanställa uppgifter ett avsevärt mindre hot mot den personliga integriteten än lagring i ett system för automatiserad behandling av personuppgifterna. Utvecklingen inom de aktuella verksamheterna går dessutom mot att behandlingen av personuppgifter i allt större utsträckning bedrivs automatiserat. I den – med tiden

alltmer begränsade – utsträckning personuppgifter lagras i traditionella pappersbaserade system kan därför inte sådana integritetsskyddsintressen anses föreligga att det finns anledning att införa några särskilda gallringsföreskrifter. För dessa handlingar kommer följaktligen endast arkivlagens bestämmelser att gälla.

När personuppgifter behandlas automatiserat uppstår helt andra möjligheter att söka och sammanställa information, vilket ökar risken för integritetskränkningar. I fråga om sådan behandling av personuppgifter är det med hänsyn till integritetsintresset nödvändigt att ha regler om gallring. Det kan inte anses tillräckligt att tillgodose skyddet för den personliga integriteten genom t.ex. sekretessbestämmelser. Sådana utgör visserligen en viss garanti för att känsliga personuppgifter inte når utanför myndigheterna. De minskar dock inte det intryck av integritetskränkning som kan framkallas hos den enskilde genom vetskapen om att känsliga personuppgifter kan behandlas automatiserat i myndighetens verksamhet under lång tid.

Sammanfattningsvis får integritetsskyddsintresset anses överväga framför de argument som anförts av Utredningen och de remissinstanser som tillstyrkt förslaget i betänkandet. Det föreslås därför att gallring som huvudregel skall ske av personuppgifter som behandlas automatiserat.

Gallringsbestämmelsens utformning

Vid utformningen av gallringsbestämmelserna måste beaktas de krav som verksamheten ställer. Den tidsram för gallring om tio år som anges i 16 § förordningen (2001:703) om viss behandling av personuppgifter inom Försvarsmakten och Försvarets radioanstalt har visat sig otillräcklig. I de aktuella verksamheterna kan uppstå behov av att med hänsyn till verksamheternas ändamål spara uppgifter under mycket lång tid. I försvarsunderrättelseverksamhet kan det förekomma att uppgifter som är så gamla som 40–70 år kan ha betydelse för bedömningar i frågor som rör den svenska utrikes-, försvars- och säkerhetspolitiken. Det kan t.ex. gälla biografiska underrättelser om militära befattningshava-

re där det i inledningen av personens karriär inhämtas uppgifter vilkas betydelse för verksamheten i framtiden då inte kan förutses. På motsvarande sätt kan uppgifter om en politisk maktbävar under personens hela livstid – och i vissa fall även därefter – vara av värde bl.a. vid en tillbakablickande studie av utvecklingen i en viss stat. Även i dessa fall är det omöjligt att i förväg veta vilka uppgifter som kan vara viktiga för verksamheten i framtiden. I den militära säkerhetstjänsten måste uppgifter om en anställd som genomgått registerkontroll kunna behandlas under hela anställningstiden, som kan uppgå till mer än 40 år. Dessa för de aktuella verksamheterna speciella förhållanden medför att utformningen av gallringsbestämmelserna kräver noggranna överväganden.

Ovan har exemplifierats hur verksamheten i vissa fall ställer krav på mycket långa bevarandetider. Naturligtvis förekommer också personuppgifter som kan gallras på ett betydligt tidigare stadium. Ett alternativ vore därför att föreskriva om olika gallringstider för olika kategorier av uppgifter. En sådan lösning är emellertid lagtekniskt komplicerad, inte minst ter det sig svårt att definiera olika uppgiftskategorier. Inte heller framstår det som en framkomlig väg att koppla gallringsföreskrifterna till de olika verksamheterna (försvarsunderrättelseverksamhet respektive militär säkerhetstjänst hos Försvarmakten och försvarsunderrättelseverksamhet respektive utvecklingsverksamhet hos Försvarets radioanstalt). Inom en verksamhet kan förekomma uppgifter med högst varierande krav på bevarandetid. En sådan uppdelning skulle därför endast leda till att mycket långa gallringstider fick anges för flertalet av verksamheterna, alternativt att föreskrifter om kortare gallringsfrister förses med omfattande undantag.

Gallringsföreskrifter med bestämda tidsramar inom vilka gallring skall ske, motsvarande vad som vanligen förekommer i särskilda registerförfattningar, framstår mot den ovan angivna bakgrunden inte som helt ändamålsenliga för de aktuella verksamheterna.

Ett alternativ till att ange bestämda gallringsfrister är att anknyta till personuppgiftslagens bestämmelse att en uppgift inte skall bevaras under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. Exempel på en sådan lösning finns i lagen (2003:763) om behandlingen av personuppgifter i socialförsäkringens administration, där det i 28 § föreskrivs att personuppgifter som behandlas automatiserat skall gallras när de inte längre är nödvändiga för de ändamål som anges i lagen, samt att regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om att personuppgifter får bevaras för historiska, statistiska och vetenskapliga ändamål. Utformningen av bestämmelsen har motiverats bl. a. med de behov av långa bevarandetider som gäller i socialförsäkringens administration (prop. 2002/03:135 s. 117 ff.). Modellen mötte viss kritik från Lagrådet som ansåg regeln vara alltför vag (aa s. 165 f.) och ifrågasatte om den tillförde något utöver vad som följer av personuppgiftslagen. Regeringen ansåg dock att en gallringsregel som anknyter till ändamålet med behandlingen, istället för bestämda tidsfrister, var tillräcklig för att tillgodose integritetsskyddsintresset. I fråga om de nu aktuella lagarna kan konstateras att personuppgiftslagens regler inte automatiskt gäller om inte annat är bestämt, till skillnad från vad som gäller enligt lagen (2003:763) om behandlingen av personuppgifter i socialförsäkringens administration. Lagrådets kritik i den delen som rör gallringsbestämmelsens förhållande till motsvarande regel i personuppgiftslagen träffar därför inte den här valda lagtekniska lösningen.

Mot bakgrund av vad som anförts om de aktuella verksamheternas speciella förutsättningar föreligger goda skäl för att i lagarna ange en ändamålsanknuten gallringsbestämmelse som huvudregel och inte i lag föreskriva om fasta tidsfrister. Det kan dock i vissa fall finnas förutsättningar för att ange bestämda – och relativt korta – tidsfrister. Eftersom gallringsbestämmelser med bestämda tidsfrister får anses innebära tydligare och mer konkreta krav på gallring än den föreslagna huvudregeln bör en möjlighet för regeringen att meddela sådana föreskrifter införas.

Lagarnas huvudregel bör därför kompletteras med ett bemyndigande för regeringen att meddela föreskrifter om att gallring skall ske senast vid viss tidpunkt.

En gallringsbestämmelse som anknyter till ändamålen med behandlingen innefattar inte samma tydliga incitament för myndigheterna att genomföra gallring av personuppgifter som om specifika gallringsfrister föreskrivs. Den föreslagna ordningen förutsätter att myndigheterna utarbetar rutiner för återkommande genomgångar av de personuppgifter som behandlas och för bedömning av när personuppgifter inte längre behövs för ändamålen med verksamheten och därför kan gallras. Verksamheternas speciella art utgör hinder för utomstående kontroll av att sådana genomgångar och bedömningar äger rum kontinuerligt. Hur gallringen organiseras samt omfattningen och utfallet av denna bör därför omfattas av den särskilda granskning som närmare beskrivs i avsnitt 8.16.

Undantag från gallring

Om en gallringsbestämmelse med föreslaget innehåll inte kompletteras med undantagsregler kommer bevarande att ske utslutande med beaktande av verksamhetens behov. I vissa fall kan det dock finnas anledning att bevara även sådana personuppgifter som inte längre behövs för verksamheten under en längre tid än vad gallringsbestämmelserna medger. En längre bevarandetid kan t.ex. motiveras av intresset att tillgodose behovet av källmaterial som underlag för historisk forskning eller andra vetenskapliga ändamål (jfr 9 § tredje stycket personuppgiftslagen). I många särskilda registerförfattningar finns också bestämmelser om undantag från gallringsföreskrifterna för mer eller mindre precist angivna ändamål. Det står klart att sådana behov av undantag föreligger också i fråga om de nu aktuella personuppgifterna. Gallringsbestämmelsen bör därför kompletteras med en regel om att regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om att personuppgifter får bevaras för hi-

storiska, statistiska och vetenskapliga ändamål. I förordning skall anges att Riksarkivet får meddela de föreskrifter som behövs.

I 8 § andra stycket första meningen personuppgiftslagen anges att bestämmelserna i lagen inte hindrar att en myndighet arkiverar och bevarar allmänna handlingar eller att arkivmaterial tas om hand av en arkivmyndighet. Regeringen uttalade i samband med personuppgiftslagens tillkomst att det inte kan anses oförenligt med en myndighets primära hantering av personuppgifter att – under förutsättning att den primära hanteringen är tillåten – bevara uppgifterna. Regeringen uttalade vidare att det inte heller kan anses oförenligt med de ursprungligen angivna ändamålen att myndigheten efter en tid lämnar över sina handlingar till en arkivmyndighet för långtidsförvaring (prop. 1997/98:44 s. 47 f). Myndigheterna är rättsligt förpliktade att bevara allmänna handlingar och bevarandet är, enligt vad regeringen uttalade, också en arbetsuppgift av allmänt intresse. Regeringen ansåg att undantagen för arkivering och bevarande i förslaget till personuppgiftslag var av väsentlig betydelse för offentlighetsprincipen och att det dessutom var ett viktigt allmänt intresse i sig att de syften som ligger till grund för arkiven kan tillgodoses.

Eftersom det i de nu föreslagna lagarna tas in bestämmelser om gallring behövs inte någon motsvarighet till 8 § andra stycket första meningen personuppgiftslagen. I den utsträckning gallring inte skall ske får personuppgifterna arkiveras eller lämnas över till en arkivmyndighet, vilket som nämnts inte kan anses oförenligt med de ursprungligen bestämda ändamålen med behandlingen.

8.21 Utlämnande av uppgifter

8.21.1 Sekretess och utlämnande av uppgifter till utländsk myndighet eller internationell organisation

Bedömning: Bestämmelser utöver vad som framgår av 1 kap. 3 § tredje stycket sekretesslagen (1980:100) om förutsättningarna för utlämnande av uppgifter för vilka sekretess gäller till en ut-

ländsk myndighet eller en internationell organisation behöver inte meddelas i lag utan kan regleras i förordning.

Utredningens bedömning överensstämmer med promemori-ans.

Remissinstanserna har inte något att invända

Skäl för bedömningen: Enligt 1 kap. 3 § tredje stycket sekretesslagen (1980:100) får uppgift för vilken sekretess råder inte röjas för utländsk myndighet eller mellanfolklig organisation annat än om utlämnande sker i enlighet med särskild föreskrift därom i lag eller förordning eller om uppgiften i motsvarande fall skulle få utlämnas till svensk myndighet och det enligt den utlämnande myndighetens prövning står klart, att det är förenat med svenska intressen att uppgiften lämnas till den utländska myndigheten eller mellanfolkliga organisationen.

Uppgifter som behandlas i Försvarmaktens underrättelse- och säkerhetstjänst och i Försvarets radioanstalts underrättelseverksamhet omfattas i stor utsträckning av sekretess av olika grad. Enligt 2 kap. 1 § sekretesslagen gäller sekretess för uppgift som angår Sveriges förbindelser med annan stat eller i övrigt rör annan stat, mellanfolklig organisation, myndighet, medborgare eller juridisk person i annan stat eller statslös, om det kan antas att det stör Sveriges mellanfolkliga förbindelser eller på annat sätt skadar landet om uppgiften röjs. Enligt 2 § samma kapitel gäller sekretess för uppgift som angår verksamhet för att försvara landet eller planläggning eller annan förberedelse av sådan verksamhet eller som i övrigt rör totalförsvaret, om det kan antas att det skadar landets försvar eller på annat sätt vållar fara för rikets säkerhet om uppgiften röjs.

I myndigheternas verksamhet finns ett behov av att kunna lämna ut även sådana uppgifter för vilka sekretess gäller till utländska samarbetspartners. En bestämmelse som ger sådan möjlighet återfinns i dag i 5 § förordningen (2001:703) om viss behandling av personuppgifter inom Försvarmakten och Försvarets radioanstalt. Bestämmelsen har sekretessbrytande karaktär

och reglerar inte på vilket sätt uppgifterna får lämnas ut, dvs. om det får ske genom utlämnande på papper eller i elektronisk form.

För att även fortsättningsvis skapa goda förutsättningar för internationellt samarbete inom underrättelse- och säkerhetstjänsten bör även det nya regelverket innehålla en bestämmelse motsvarande 5 § i förordningen om viss behandling av personuppgifter inom Försvarmakten och Försvarets radioanstalt. I syfte att undvika detaljreglering i lagarna och skapa utrymme för långsiktig flexibilitet bör den närmare regleringen av förutsättningarna för sådant utlämnande liksom hittills ske i förordningsform. Något konstitutionellt hinder mot att regeringen genom förordning medger att annars sekretessbelagda uppgifter lämnas ut myndigheter emellan föreligger inte, såvida inte sådant uppgiftsutbyte regleras exklusivt i lag.

8.21.2 Utlämnande av personuppgifter på medium för automatiserad behandling

Förslag: Enstaka personuppgifter får lämnas ut på medium för automatiserad behandling. Annars får utlämnande på sådant medium ske endast om regeringen har meddelat föreskrifter eller beslut om det.

Utredningens förslag innebär att utlämnande av personuppgifter på medium för automatiserad behandling inte skall regleras särskilt.

Remissinstanserna har inte något att invända

Skäl för förslaget: Uppgifter från den militära underrättelse- och säkerhetstjänsten eller Försvarets radioanstalt kan lämnas ut på traditionellt sätt i muntlig eller skriftlig form. Utlämnande kan också ske i elektronisk form på medium för automatiserad behandling, t.ex. genom användning av e-post, genom utlämnande på diskett eller cd-rom, eller genom direktåtkomst. Direktåtkomst behandlas i avsnitt 8.21.3. Utlämnande på medium för automatiserad behandling innebär som regel att informationen

lämnas ut i elektronisk form på ett sådant sätt att mottagaren kan bearbeta informationen.

Av såväl dataskyddsdirektivet som personuppgiftslagen framgår att uppgifter skall samlas in för särskilda, uttryckliga och berättigade ändamål samt att senare behandling inte får ske på ett sätt som är oförenligt med dessa ändamål (9 § första stycket c och d personuppgiftslagen). En uppgift som har samlats in för ett visst ändamål får följaktligen inte lämnas ut, om utlämnandet är oförenligt med det ursprungligen angivna ändamålet. Data-skyddsdirektivet är visserligen inte tillämpligt på de aktuella verksamheterna hos Försvarsmakten och Försvarets radioanstalt men direktivets och personuppgiftslagens bestämmelser i denna del bör i så stor utsträckning som möjligt tillämpas för de båda myndigheterna. Utlämnande av personuppgifter får därför endast ske när detta inte är oförenligt med de olika ändamål som gäller för behandling av personuppgifterna. Varken dataskyddsdirektivet eller personuppgiftslagen reglerar närmare om eller under vilka förutsättningar uppgifter som omfattas av direktivets eller lagens tillämpningsområde får lämnas ut automatiserat.

I Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst och i Försvarets radioanstalts underrättelse- och utvecklingsverksamhet aktualiseras med hänsyn till verksamheternas art i huvudsak utlämnande på medium för automatiserad behandling till annan svensk myndighet och till annan stat eller internationell organisation inom ramen för det internationella underrättelse- och säkerhetssamarbetet. Sekretessnivån är i övrigt sådan att utlämnande av uppgifter sällan kommer i fråga.

Av det förslag till ändringar i lagen (2000:130) om försvarsunderrättelseverksamhet som presenteras i Ds 2005:30 framgår att underrättelser – som i vissa fall kan innehålla personuppgifter – skall rapporteras till regeringskansliet och andra berörda myndigheter. I det internationella samarbetet sker utlämnande med stöd av den i föregående avsnitt behandlade föreskriften. I detta sammanhang ställs med hänsyn till verksamheternas art mycket höga säkerhetskrav för att utlämnande skall få ske. Kan dessa

säkerhetskrav inte efterlevs, sker inte utlämnande på medium för automatiserad behandling, utan i stället t.ex. i pappersform.

En viktig utgångspunkt för en ny reglering är att Försvarsmakten och Försvarets radioanstalt skall kunna utnyttja automatiserade förfaranden och i övrigt bedriva de aktuella verksamheterna med ett rationellt datorstöd, samtidigt som risken för otillbörliga intrång i enskildas personliga integritet minimeras. Med hänsyn till att det i praktiken inte behöver vara så stora skillnader mellan direktåtkomst och utlämnande på medium för automatiserad behandling bör dock båda formerna av elektroniskt utlämnande författningsregleras. Att till en mottagare dagligen på medium för automatiserad behandling, t.ex. e-post, översända en hel databas liknar nämligen i praktiken en direktåtkomst till databasen. För att förenkla för myndigheterna och med hänsyn till den stränga sekretess som normalt gäller bör dock utlämnande av enstaka personuppgifter på medium för automatiserad behandling, t.ex. via e-post, kunna tillåtas. I övrigt bör det ankomma på regeringen att ange när utlämnande på medium för automatiserad behandling får ske.

8.21.3 Direktåtkomst

Förslag: Vilka som får ha direktåtkomst till personuppgifter bestäms av regeringen i förordning eller beslut.

Regeringen, eller den myndighet regeringen bestämmer, meddelar närmare föreskrifter eller beslut om omfattningen av direktåtkomsten.

Utredningens förslag innebär att direktåtkomst endast regleras såvitt avser uppgifter i databaser.

Remissinstanserna har inte något att erinra mot lagförslagen men har anfört synpunkter på vilka myndigheter som i förordning skall ges möjlighet till direktåtkomst.

Skälen för förslaget: I personuppgiftslagen finns inte några bestämmelser som reglerar möjligheten till direktåtkomst till uppgifter som behandlas automatiserat. Direktåtkomst innebär

att någon har direkt tillgång till en uppgiftssamling och kan söka efter information i denna, utan att kunna påverka innehållet i uppgiftssamlingen. Mottagare med direktåtkomst kan i regel också kopiera informationen och därefter bearbeta den. Informationsöverföringen sker utan att den myndighet som ansvarar för uppgiftssamlingen i det enskilda fallet tar ställning till om informationen skall lämnas ut. I många registerförfattningar och andra författningar om behandling av personuppgifter finns bestämmelser som reglerar direktåtkomst till myndigheters uppgiftssamlingar.

Myndigheters möjlighet att ta del av varandras information genom direktåtkomst begränsas av sekretesslagens bestämmelser. Direktåtkomst innebär att den myndighet som har sådan åtkomst fritt kan avgöra vilka uppgifter den vill ta del av. Om en myndighet har direktåtkomst till uppgifter får dessa därför anses utlämnade i och med att ett system för direktåtkomst upprättats. Det saknar därvid betydelse om myndigheten faktiskt använder sig av en viss uppgift eller inte. Om uppgifter i en uppgiftssamling omfattas av sekretess som innebär att den myndigheten som har direktåtkomst vid en prövning enligt sekretesslagen inte med säkerhet skulle ha rätt att ta del av uppgifterna, bör myndigheten därför inte heller kunna få direktåtkomst till en uppgiftssamling.

Mot ovanstående bakgrund bör direktåtkomst endast komma i fråga avseende uppgifter för vilka det inte är föreskrivet sekretess, uppgifter som enligt lag eller förordning skall lämnas ut till den som har direktåtkomst (se 14 kap. 1 § sekretesslagen) eller uppgifter som med stöd av generalklausulen i 14 kap. 3 § sekretesslagen får lämnas ut rutinmässigt efter en på förhand gjord intresseavvägning.

Avsikten med bestämmelserna om direktåtkomst i lagarna är att sådan åtkomst skall komma i fråga dels om de aktuella uppgifterna inte omfattas av sekretess och dels om det finns en skyldighet enligt sekretesslagen eller annan lag eller förordning att lämna ut de aktuella uppgifterna till den som får ha direktåtkomst. Någon generell sekretessbrytande verkan är inte avsedd. Det har i olika sammanhang diskuterats om bestämmelser enligt

vilka någon skall ha direktåtkomst generellt skall anses innebära att de bryter sekretess för de uppgifter till vilka det föreskrivs direktåtkomst (se t.ex. prop. 2001/01:33, s. 131 och 347f.). För att markera att så inte skall vara fallet i fråga om de nu aktuella bestämmelserna föreslås att det i författningarna om behandling av uppgifter i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst samt i Försvarets radioanstalts underrättelse- och utvecklingsverksamhet anges att någon *får* ha direktåtkomst.

Bedömningen av vilka som skall få ha direktåtkomst måste göras efter en avvägning mellan hänsynen till å ena sidan myndigheternas effektivitet och å andra sidan de registrerades integritet. Vid denna avvägning måste också beaktas den sekretess och säkerhet i övrigt som gäller inom de aktuella verksamheterna. Av verksamhetens karaktär följer också att det är ett grundläggande krav att myndigheternas information inom såväl försvarsunderrättelseverksamheten som säkerhetstjänsten inte sprids till obehöriga.

I andra registerförfattningar anges vanligen i lag vilka myndigheter som får ha direktåtkomst, medan det överläts till regeringen att närmare bestämma omfattningen av sådan direktåtkomst. Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst samt Försvarets radioanstalts underrättelse- och utvecklingsverksamhet är dock av sådan karaktär att det inte är självklart att samma lösning skall väljas för dessa verksamheter, i synnerhet försvarsunderrättelseverksamheten. I avsnitt 7.1 presenteras en rad skäl för varför det inte är lämpligt att detaljreglera denna verksamhet i lag. Dessa skäl gör sig gällande även i fråga om regleringen av direktåtkomst. I promemorian föreslås därför att regeringen genom förordning eller särskilt beslut får bestämma vilka myndigheter som får ha direktåtkomst. Regeringen eller den myndighet regeringen bestämmer bör även få meddela närmare föreskrifter eller beslut om omfattningen av direktåtkomsten.

8.22 Bestämmelser i personuppgiftslagen som inte upprepas

Bedömning: Utöver de bestämmelser i personuppgiftslagen som behandlas i avsnitt 8.4, 8.11, 8.14, 8.15, 8.17, 8.18 och 8.19 skall bestämmelser motsvarande de i 4-7, 21 och 29 §§ personuppgiftslagen inte återfinnas i lagförslagen.

Utredningen berör inte särskilt de bestämmelser i personuppgiftslagen som inte tillämpas.

Remissinstanserna: -

Skäl: I avsnitt 8.4, 8.11, 8.14, 8.15, 8.17, 8.18 och 8.19 har re-
dovisats skälen till varför vissa bestämmelser i personuppgiftslagen (1998:204) inte skall gälla för behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst och Försvarets radioanstalts underrättelseverksamhet. Därutöver kommer följande bestämmelser i personuppgiftslagen inte att gälla för behandling av personuppgifter i dessa verksamheter.

Det territoriella tillämpningsområdet

I 4 § personuppgiftslagen anges att lagen gäller för sådan personuppgiftsansvariga som är etablerade i Sverige eller som är etablerade i tredje land, men som för behandlingen av personuppgifter använder sig av utrustning som finns i Sverige.

Lagförslagen i denna promemoria omfattar endast Försvarmakten och Försvarets radioanstalt, varför bestämmelsen är obehövlig.

Undantag för privat behandling av personuppgifter

Personuppgiftslagen gäller enligt 6 § inte för sådan behandling av personuppgifter som en fysisk person utför som ett led i en verksamhet av rent privat natur.

Bestämmelsen är inte tillämplig i de verksamheter som omfattas av promemorian.

Förhållandet till tryck- och yttrandefriheten

I 7 § första stycket personuppgiftslagen finns en upplysning om att bestämmelserna i lagen inte tillämpas i den utsträckning det skulle strida mot bestämmelserna om tryck- och yttrandefrihet i tryckfrihetsförordningen eller yttrandefrihetsgrundlagen. Bestämmelser i vanlig lag kan inte ta över bestämmelser i grundlag. Bestämmelserna om tryck- och yttrandefrihet i tryckfrihetsförordningen eller yttrandefrihetsgrundlagen gäller således framför personuppgiftslagen (1998:204) och de i denna promemoria föreslagna lagarna.

I samband med personuppgiftslagens tillkomst uttalade regeringen att lagtexten i syfte att klargöra och underlätta tillämpningen borde innehålla en uttrycklig erinran om att bestämmelserna i personuppgiftslagen inte skall tillämpas om en sådan tillämpning skulle strida mot bestämmelserna om tryck- och yttrandefrihet i tryckfrihetsförordningen eller yttrandefrihetsgrundlagen. Enligt regeringen var en sådan erinran viktig för att inskräpa att tillämpningen vid fall av möjliga konflikter skall präglas av försiktighet och respekt för det grundlagsskyddade området (prop. 1997/98:44 s. 51 f.).

7 § andra stycket innebär att vissa närmare angivna bestämmelser i personuppgiftslagen inte skall tillämpas på sådan behandling av personuppgifter som sker uteslutande för journalistiska ändamål eller konstnärligt eller litterärt skapande. Eftersom grundlagsskyddade förfaranden omfattas av paragrafens första stycke berör denna bestämmelse förfaranden som inte åtnjuter sådant skydd.

Bestämmelsen i paragrafens första stycke utgör endast en påminnelse om vad som ändå gäller. Den verksamhet som berörs av de föreslagna lagarna innefattar inte sådana förfaranden som omfattas av bestämmelsen i andra stycket. Det finns därför inte an-

ledning att införa motsvarande bestämmelser i de föreslagna lagarna.

Uppgifter om lagöverträdelser

Bestämmelsen i 21 § personuppgiftslagen innehåller ett förbud för andra än myndigheter att behandla personuppgifter om lagöverträdelser. Det är således tillåtet för myndigheter att behandla domar m.m., varför en motsvarande bestämmelse är överflödig.

Automatiserade beslut

Om ett beslut som har rättsliga följder för en fysisk person eller annars har märkbara verkningar för den fysiska personen, grundas enbart på automatiserad behandling av sådana personuppgifter som är avsedda att bedöma egenskaper hos personen, skall den som berörs av beslutet ha möjlighet att på begäran få beslutet omprövat av någon person, 29 § personuppgiftslagen.

Varken Försvarsmakten eller Försvarets radioanstalt fattar sådana beslut i de verksamheter som regleras i denna promemoria. En bestämmelse motsvarande den i personuppgiftslagen behövs därför inte.

9 Särskilda bestämmelser för samlingar av uppgifter

9.1 Samlingar av uppgifter

Förslag: Inom Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst samt Försvarets radioanstalts underrättelse- och utvecklingsverksamhet skall det få finnas samlingar av uppgifter som med hjälp av automatiserad behandling används gemensamt i respektive verksamhet för de i lagarna angivna ändamålen. Vilka uppgiftssamlingar som får finnas hos myndigheterna skall regleras i förordning.

Utredningens förslag innebär att det i lagen skall anges vilka databaser som skall finnas hos myndigheterna, men överensstämmer i övrigt i huvudsak med promemorians förslag.

Remissinstanserna: De flesta remissinstanserna tillstyrker eller har inget att invända mot att samlingar av uppgifter regleras särskilt och att begreppet databas används för att beteckna sådana samlingar. *Säkerhetspolisen* ställer sig emellertid tveksam till om det är lämpligt att i lagen peka ut vilka databaser som får finnas, eftersom detta gör lagstiftningen mindre flexibel. Säkerhetspolisen är också tveksam till uppdelningen av uppgifter beroende på deras tillgänglighet och anser att gränsdragningen bör ske mellan behandling av personuppgifter för det avsedda ändamålet och inledande tillfällig behandling.

Skäl för förslaget:

Användningen av datorer är ett naturligt och omfattande inslag i den militära underrättelse- och säkerhetstjänstens arbete. För Försvarets radioanstalts underrättelseverksamhet är sådan hantering av uppgifter den helt dominerande arbetsmetoden. Inom de båda myndigheternas verksamheter pågår kontinuerligt en utveckling mot allt mer avancerade datorsystem.

Ett dominerande inslag i verksamheterna är sådan automatiserad och gemensam behandling av personuppgifter som inte utgörs av vanlig ordbehandling och som inte är av helt tillfällig natur. På grund av de tekniska möjligheterna att söka i materialet och göra sammanställningar av behandlade personuppgifter utgör sådan behandling en påtaglig risk för intrång i enskildas personliga integritet. Integritetsskyddsintresset motiverar därför att det införs en särskild reglering av vilka gemensamt använda samlingar av uppgifter som får förekomma i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst samt Försvarets radioanstalts underrättelse- och utvecklingsverksamhet.

I datalagen (1973:289) användes begreppet personregister, men i och med genomförandet av dataskyddsdirektivet i svensk lagstiftning ändrades den rättsliga begreppsapparaten vid datoranvändning, och i personuppgiftslagen talas i stället om behandling av personuppgifter. Utredningen har i syfte att särskilja den rättsliga regleringen av sådan automatiserad behandling som i dag görs i uppgiftssamlingar för gemensamt bruk, t.ex. personregister, från den automatiserade behandlingen av uppgifter i allmänhet, t.ex. ordbehandling och vanlig e-posthantering, föreslagit att begreppet databas används i lagstiftningen. Databas är ett allmänt vedertaget begrepp som inom Försvarmakten och Försvarets radioanstalt används för att beteckna uppgiftssamlingar och som också förekommer i många registerförfattningar. Emellertid bör den lagstiftning som nu föreslås vara helt teknikneutral och inte i onödan binda myndigheterna vid användandet av vissa begrepp. Det kan inte uteslutas att utvecklingen efterhand gör att användande av begreppet databas medför att myndigheterna finner sig bundna till vissa tekniska system. I promemorian föreslås därför att den helt neutrala beteckningen uppgiftssamling skall användas.

Gränsdragningen mellan gemensam behandling i en uppgiftssamling och annan behandling av uppgifter

För att en särskild reglering av samlingar av uppgifter skall vara möjlig är det nödvändigt att dra gränsen mellan behandling i en sådan uppgiftssamling och annan behandling, t.ex. vanlig ordbehandling. En grundläggande förutsättning för att en uppgift som behandlas automatiserat skall anses ingå i en uppgiftssamling är att uppgiften används gemensamt i en viss verksamhet för de ändamål som styr behandlingen av uppgifter inom verksamheten.

En uppgift används gemensamt och utgör därmed en del av en uppgiftssamling om den behandlas på ett sätt som medför att den är allmänt tillgänglig i verksamheten. Olika begränsningar av åtkomsten till uppgifter, t.ex. genom krav på viss behörighet, kan i praktiken medföra att uppgifter endast är åtkomliga för ett begränsat antal personer. Detta hindrar dock inte att uppgifterna kan betraktas som gemensamt tillgängliga.

I samband med att en tjänsteman arbetar med ordbehandling lagras uppgifter elektroniskt på hårddisken i en dator eller i en server hos Försvarmakten eller Försvarets radioanstalt. Uppgiften är då normalt åtkomlig endast för tjänstemannen själv och exempelvis systemadministratören vid myndigheten. En sådan uppgift kan därför inte anses vara gemensamt tillgänglig. Syftet med sådan tillfällig behandling är inte att uppgifterna som lagras i datorn skall användas av andra än den som utför behandlingen. När en uppgift behandlas tillfälligt i en dator för att senare tillföras en uppgiftssamling och göras gemensam utgör den inte heller en del av uppgiftssamlingen förrän den väl införts i det gemensamma systemet.

Den snabba tekniska utvecklingen medför ständigt nya möjligheter i fråga om informationsöverföring och det är därför inte möjligt att i lagstiftningen ange någon exakt gräns för när en viss behandling skall anses ske i en uppgiftssamling och därmed omfattas av de särskilda bestämmelser som reglerar sådana samlingar. Myndigheterna måste i det enskilda fallet avgöra om uppgifter som behandlas automatiserat är gemensamma eller inte. En tjänsteman inom Försvarmakten eller Försvarets radioanstalt

torde i regel utan svårigheter kunna avgöra om han eller hon för tillfället arbetar med en uppgift direkt i en uppgiftssamling eller i ett ordbehandlingsdokument. Den personuppgiftsansvarige har ett ansvar för att gränsdragningsproblem inte uppstår på grund av brister i den tekniska utformningen av ett datorsystem. Genom de höga säkerhetskrav som omgärdar Försvarmaktens och Försvarets radioanstalts datorsystem är det också nödvändigt att verksamheten ha klart för sig huruvida en viss uppgift ingår i en uppgiftssamling eller inte.

Avgörande för när automatiserat behandlade uppgifter skall anses ingå i en uppgiftssamling bör sammanfattningsvis vara att uppgifterna av Försvarmakten eller Försvarets radioanstalt används gemensamt i en viss verksamhet för de ändamål som skall styra behandlingen av uppgifter inom verksamheten. Denna avgränsning skall framgå av lagtexten.

Säkerhetspolisen har anfört att gränsdragningen i stället bör ske mellan behandling av personuppgifter för det avsedda ändamålet och inledande tillfällig behandling. Genom en sådan gränsdragning skulle dock all behandling av personuppgifter utom den inledande, som syftar till att avgöra om uppgiften behövs för ändamålet, falla under den särskilda regleringen. Sådan behandling kan dock ske i olika former och något behov av en särskild reglering kan inte anses råda i alla behandlingssituationer.

Uppgiftssamlingarna skall regleras i förordning

Förutsättningarna för bedrivandet av Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt Försvarets radioanstalts underrättelse- och utvecklingsverksamhet förändras ständigt. Dels påverkar förändringar i omvärlden verksamhetens inriktning och fokus, dels medför den tekniska utvecklingen nya möjligheter att insamla och bearbeta information. För att målen med verksamheterna skall kunna uppfyllas på ett effektivt och rationellt sätt erfordras ett stort mått av flexibilitet och förmåga till omvärlds Anpassning. Detta ställer också krav på de regelverk som styr verksamheten. Lagar och förord-

ningar måste ge nödvändigt utrymme för anpassning av verksamheten efter ändrade förhållanden samtidigt som regleringarna skall vara förutsebara och erbjuda ett fullgott skydd för enskildas integritet. Mot den bakgrunden bör det noga övervägas om ett visst förhållande skall regleras i lag eller om föreskrifter istället kan meddelas i förordning.

Som *Säkerhetspolisen* framhållit medför ett direkt utpekande i lag av vilka uppgiftssamlingar som får finnas att lagstiftningen blir mindre flexibel. En sådan ordning innebär att nya uppgiftssamlingar inte kan tillkomma eller befintliga avvecklas eller förändras till sitt innehåll utan en utdragen lagstiftningsprocedur. Dessa nackdelar talar med styrka för att en alltför detaljerad reglering i lag bör undvikas. Ur integritetsskyddsperspektiv framstår det dock inte heller som lämpligt att helt överlåta frågan om vilka uppgiftssamlingar som skall få inrättas till myndigheterna. Den närmare regleringen av vilka uppgiftssamlingar som skall få finnas hos myndigheterna bör följaktligen ske i förordning.

9.2 Uppgifter som får behandlas

Förslag: Regeringen meddelar närmare föreskrifter om vilka uppgifter som får behandlas i Försvarsmaktens och Försvarets radioanstalts uppgiftssamlingar.

Utredningens förslag överensstämmer i allt väsentligt med promemorians. Utredningen har dock i förslaget till lag om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänsten föreslagit en hänvisning till den bestämmelse om behandling av personuppgifter i militär säkerhetstjänst som motsvarar 1 kap. 9 § i den här föreslagna lagen.

Remissinstanserna tillstyrker eller har inget att invända mot förslagen. *Hovrätten för Övre Norrland* ställer sig tveksam till nödvändigheten av en bestämmelse som endast utgör en upplysning om vad som följer av en annan bestämmelse.

Skälen för förslaget: Som redovisats i avsnitt 7.1 bör en lag om behandling av personuppgifter endast slå fast grundläggande principer för behandlingen och inte i detalj reglera vad som får behandlas. De verksamheter som berörs av promemorians förslag är av sådan art att det inte är möjligt att i lagform reglera behandlingen av uppgifter i detalj. Behovet av detaljerade integritetsskyddsbestämmelser i lagarna måste dessutom ställas i relation till att skyddet för den personliga integriteten på detta område i hög grad tillgodoses genom den särskilda kontroll som beskrivs i avsnitt 8.16 samt genom att verksamheterna i stora delar är hemliga och att de personuppgifter som behandlas därför omgärdas av sekretess. Dessutom ställs i verksamheterna mycket höga krav på bl.a. datasäkerhet och säkerhetsåtgärder när det gäller spridning av uppgifter till utomstående.

Den yttre ramen för vilka uppgifter som får behandlas begränsas genom de i lagförslagen angivna ändamålen. Den närmare regleringen av vilka kategorier av uppgifter som skall få behandlas bör med hänsyn till vad som anförts ovan återfinnas i förordning eller regeringsbeslut.

Bestämmelser om under vilka förutsättningar personuppgiftsbehandling överhuvudtaget är tillåten i de olika verksamheterna återfinns i lagarnas 1 kap. Det finns inte anledning att också i anslutning till bestämmelserna om uppgifter i samlingar upplysa om detta. Som *Hovrätten för Övre Norrland* anført behövs därför inte den av utredningen föreslagna hänvisningen till vilka uppgifter som får behandlas i den militära säkerhetstjänsten.

10 Ikraftträdande och övergångsbestämmelser

Förslag: Lagen om behandling av uppgifter i Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten och lagen om behandling av uppgifter i Försvarets radioanstalts underrättelseverksamhet skall träda i kraft den 1 januari 2007.

Samtidigt med att de nya lagarna träder i kraft skall den förordning som i dag reglerar behandlingen av personuppgifter inom Försvarmakten och Försvarets radioanstalt upphöra att gälla.

Bestämmelser i de nya lagarna om grundläggande krav på behandling av personuppgifter samt behandling av känsliga personuppgifter skall inte börja tillämpas förrän den 1 oktober 2007 i fråga om sådan manuell behandling av personuppgifter, som påbörjats före den 24 oktober 1998, eller manuell behandling av personuppgifter, som utförs för ett visst bestämt ändamål, om manuell behandling för ändamålet påbörjats före den 24 oktober 1998.

Utredningens förslag överensstämmer med promemorians med undantag för att Utredningen föreslår att lagarna skall träda i kraft den 1 juli 2004.

Remissinstanserna: -

Skäl för förslaget: Den nya lagstiftning som föreslås för behandling av uppgifter i Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet bör kunna träda i kraft den 1 januari 2007. Detsamma gäller de nya förordningar och

förordningsändringar som föranleds av den nya lagstiftningen. Samtidigt bör förordningen (2001:703) om viss behandling av personuppgifter inom Försvarmakten och Försvarets radioanstalt upphöra att gälla.

För manuell behandling skall enligt övergångsbestämmelserna till personuppgiftslagen (1998:204) vissa bestämmelser i personuppgiftslagen inte börja tillämpas fullt ut förrän den 1 oktober 2007. De föreslagna lagarna omfattar sådan manuell behandling som i avsaknad av särskild lagstiftning skulle omfattas av personuppgiftslagens bestämmelser. Det saknas anledning att låta manuell behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet omfattas av lagstiftningen i annan utsträckning än vad som skulle ha varit fallet om endast personuppgiftslagens bestämmelser hade varit tillämpliga. De undantag från tillämpning fram till den 1 oktober 2007 som föreskrivs i personuppgiftslagen avseende manuella register, som påbörjats redan före den lagens ikraftträdande, bör därför gälla även för behandling enligt den nu föreslagna lagstiftningen. I praktiken torde dock övergångsbestämmelsen sakna eller ha mycket begränsad betydelse.

I övrigt bedöms att behandling av personuppgifter och andra uppgifter som i dag utförs i Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet utan ytterligare övergångsbestämmelser direkt kan omfattas av bestämmelserna i den nya lagstiftningen när den träder i kraft.

11 Konsekvensbeskrivning

Bedömning: Den rättsliga regleringen av behandlingen av personuppgifter som föreslås är ett resultat av att försöka finna den bästa möjliga avvägning mellan användandet av modern teknik och utveckling av sådan samt skyddet av den enskildes personliga integritet. De bestämmelser som föreslås förhindrar inte och försvårar inte en effektivisering av Försvarmaktens och Försvarets radioanstalts verksamhet. Genom att undvika en onödig detaljreglering hindras inte framtida teknikutveckling och rationaliseringar. Förslagen medför inte några kostnadsökningar.

Utredningens bedömning överensstämmer med promemorians.

Remissinstanserna tillstyrker eller har inte något att invända.

Skäl för bedömningen: En utgångspunkt har varit att föreslå moderna, teknikneutrala och allmänt ändamålsenliga bestämmelser för behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst samt i Försvarets radioanstalts underrättelse- och utvecklingsverksamhet. Särskild hänsyn har, så långt det är möjligt med hänsyn till verksamheternas art, tagits till de integritetsaspekter som följer av omfattande automatiserad behandling av personuppgifter i myndigheternas verksamhet. Förslagen är ägnade att främja det internationella försvarsunderrättelse- och säkerhetssamarbetet mellan Försvarmakten samt Försvarets radioanstalt och myndigheter i andra stater eller internationella organisationer.

Författningsförslagen kommer inte att innebära några kostnader för Försvarmaktens eller Försvarets radioanstalts pågående

verksamhet, eftersom de befintliga datorsystemen kan bibehållas. De förslagna lagarna är teknikneutrala och tillåter således att nya datorsystem i framtiden kan tillskapas utan att det blir nödvändigt att ändra lagarna.

Vissa utbildningsinsatser kan komma att krävas men dessa är jämfört med den fortlöpande vidareutbildningen av personalen inom Försvarmakten och Försvarets radioanstalt, inte mer omfattande än att de kan täckas av ordinarie ekonomiska ramar.

Enligt förslaget skall Försvarets underrättelsenämnd till skydd för den personliga integriteten få i uppgift att särskilt granska den behandling av uppgifter som sker med stöd av de författningar som föreslås. Granskningen av personuppgiftsbehandlingen kan genomföras i samband med den mycket närliggande kontroll av Försvarmaktens och Försvarets radioanstalts verksamhet som nämnden redan i dag har att utföra. Vilka konsekvenser den nämnda kontrollen och den utökade kontrollen som föreslås i Ds (Fö 2005:30) En anpassad försvarsunderrättelseverksamhet får för nämnden behandlas i den promemorian. Förslaget i denna del bör dock inte rimligen leda till några ytterligare kostnadsökningar för staten.

Förslagen bedöms inte ha några konsekvenser när det gäller kostnader eller intäkter för kommuner, landsting, företag eller andra enskilda. Inte heller bedöms förslagen ha några konsekvenser för den kommunala självstyrelsen, brottsligheten och det brottsförebyggande arbetet, sysselsättningen, den offentliga servicen i olika delar av landet, små företags arbetsförutsättningar, konkurrensförmågan eller villkor i övrigt i förhållande till större företags. Detsamma gäller jämställdheten mellan män och kvinnor och möjligheterna att nå de integrationspolitiska målen.

12 Författningskommentar

12.1 Förslag till lag om behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst

1 kap. Allmänna bestämmelser

Lagens tillämpningsområde m.m.

1 §

I *första stycket* anges lagens tillämpningsområde. Lagen är tillämplig vid behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst, 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 som är tillgänglig för sökning eller sammanställning enligt särskilda kriterier. Med personuppgifter avses detsamma som i personuppgiftslagen, nämligen all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet. Behandling av uppgifter om avlidna personer eller juridiska personer omfattas alltså inte av lagen. Vad som inbegrips i försvarsunderrättelseverksamhet och den militära säkerhetstjänsten defi-

nieras inte, men ledning kan hämtas i ändamålsbestämmelserna, se avsnitt 8.5. För behandling av personuppgifter i den interna verksamheten gäller personuppgiftslagen (1998:204). Se även avsnitt 7.3 vad gäller tillämpningsområdet.

Bestämmelserna är generella och gäller, om inte annat sägs, för all behandling av uppgifter i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst, oavsett om det gäller e-post, enskilda tjänstemäns promemorior som upprättas i ordbehandlingsprogram, mindre register som används tillfälligt i underrättelseprojekt eller större register och datorsystem som används gemensamt i verksamheterna.

För tydlighetens skull anges *i andra stycket* lagens förhållande till personuppgiftslagen. Den föreslagna lagen är heltäckande och innehåller alltså alla de bestämmelser som skall vara tillämpliga vid Försvarmaktens behandling av personuppgifter i försvarsunderrättelseverksamheten och den militära säkerhetstjänsten. Personuppgiftslagen gäller följaktligen inte vid sådan behandling. De närmare övervägandena i denna del framgår av avsnitt 7.2.

2 §

I paragrafen anges lagens syfte, som är detsamma som det i 1 § personuppgiftslagen (1998:204). Se avsnitt 7.4.

Förhållandet till offentlighetsprincipen

3 §

Bestämmelsen innehåller en upplysning, motsvarande den i 8 § första stycket personuppgiftslagen (1998:204), om att lagen inte skall tillämpas om det skulle strida mot en myndighets skyldigheter enligt 2 kap. tryckfrihetsförordningen. Se avsnitt 8.1.

Definitioner

4 §

I bestämmelsen definieras centrala begrepp i lagen. Definitionerna överensstämmer med de i personuppgiftslagen (1998:204), med undantag av begreppen samtycke och tredje land som inte används i den föreslagna lagen samt begreppen personuppgiftsansvarig respektive tillsynsmyndighet, vilkas betydelse framgår av 1 kap. 5 § och 5 kap. 1 §. Se vidare avsnitt 8.2.

Personuppgiftsansvar

5 §

I bestämmelsen tydliggörs att Försvarmakten är personuppgiftsansvarig för den personuppgiftsbehandling som sker i försvarsunderrättelseverksamheten och i den militära säkerhetstjänsten, se avsnitt 8.3. Med personuppgiftsansvaret följer en rad skyldigheter. Den personuppgiftsansvarige skall bl.a. se till att behandlingen av personuppgifter sker på ett korrekt sätt samt att information lämnas till den registrerade, se bl.a. avsnitt 8.4. I ansvaret ligger också att bestämma medlen för personuppgiftsbehandlingen och de närmare ändamålen för denna, inom ramen för de ändamål som anges i lagen.

Grundläggande krav på behandling av personuppgifter

6 §

Bestämmelsen innehåller grundläggande krav på behandling av personuppgifter och upptar delvis de krav som återfinns i 9 § personuppgiftslagen. De närmare övervägandena framgår av avsnitt 8.4.

När behandling av personuppgifter är tillåten

Försvarsunderrättelseverksamhet

7 §

Paragrafen anger de ändamål för vilka personuppgifter får användas i försvarsunderrättelseverksamheten genom en hänvisning till lagen (2000:130) om försvarsunderrättelseverksamhet. Ändamålet omfattar därmed också de förändringar som föreslås i Ds 2005:30, se vidare avsnitt 6.

Försvarsunderrättelseverksamheten är ett led i Försvarmaktens uppgifter att i fred, under beredskap och i krig ge underlag för Försvarmaktens beredskap, operativa verksamhet och förbandsproduktion samt för krigsorganisationens utveckling och materiella förnyelse. Försvarsunderrättelseverksamhet består av inhämtning, bearbetning och analys samt delgivning av information. Härigenom utarbetas underrättelser som delges Regeringskansliet och andra berörda myndigheter. Det är regeringen som bestämmer den närmare inriktningen av försvarsunderrättelseverksamheten.

Försvarsunderrättelseverksamheten skall identifiera och redovisa eller ge förvarning om sådana förändringar i omvärldsläget att detta kan ligga till grund för politiska beslut om totalförsvarets anpassning på kort eller lång sikt. Totalförsvaret är den verksamhet som behövs för att förbereda Sverige för krig och består av militär verksamhet (militärt försvar) och civil verksamhet (civilt försvar), 1 § lagen (1992:1403) om totalförsvaret och höjd beredskap.

Uppgifter behandlas för den militära underrättelsetjänstens centrala uppgift att inom ramen för Försvarmaktens grundberedskap upprätthålla försvar mot väpnat angrepp och för att hävda svensk territoriell integritet. Personuppgifter behandlas också vid behandling av uppgifter vid Sveriges deltagande vid internationella fredsbevarande och humanitära insatser, samt för att stärka samhällets förmåga att förebygga och hantera

svåra påfrestningar på samhället. Det gäller att kunna förutse konflikter samt bearbeta inhämtat material och delge bedömningar om säkerhetspolitiska och militära förhållanden. Det kan också röra sig om att medverka med information och analys i fråga om hot av annan än rent militär karaktär.

Personuppgifter behandlas också om t.ex. utländsk militär personal, politiker eller andra viktiga befattningshavare. Sådana uppgifter är nödvändiga att behandla för att informationsunderlaget till stöd för svensk utrikes-, försvars- och säkerhetspolitik skall bli komplett.

Utöver de ändamål som anges i lagen om försvarsunderrättelseverksamhet och regeringen inriktning framgår av *andra stycket* att behandlingen av personuppgifter också begränsas av att behandlingen endast får avse personer som har anknytning till en preciserad inriktning för verksamheten och att behandlingen skall vara nödvändig för att fullfölja en sådan inriktningen. Med *preciserad inriktning* avses de interna inriktningar som Försvarsmakten fastställer för närmare avgränsning av verksamheten (se vidare avsnitt 8.5).

Vilken grad av anknytning en person skall ha till en preciserad inriktning för att behandling av uppgifter om honom eller henne skall kunna anses godtagbar, måste med hänsyn till verksamhetens speciella karaktär avgöras från fall till fall. Under alla omständigheter måste det emellertid alltid finnas en sådan koppling mellan en person och den företeelse som verksamheten syftar till att kartlägga att man i efterhand kan kontrollera att personuppgiftsbehandlingen är motiverad av verksamhetsskäl och kan hänföras till en viss preciserad inriktning.

Den militära säkerhetstjänsten

8 §

Paragrafen anger de ändamål för vilka uppgifter får användas – d.v.s. samlas in registreras, lämnas ut och i övrigt behandlas – i den militära säkerhetstjänsten.

Ändamålet med behandlingen av personuppgifter inom den

militära säkerhetstjänsten är att Försvarsmakten skall kunna utföra de uppgifter som åligger myndigheten enligt säkerhetskyddslagen (1996:627), säkerhetskyddförordningen (1996:633) och 4 § 2 förordningen (2000:555) med instruktion för Försvarsmakten. Uppgifter får behandlas i Försvarsmaktens militära säkerhetstjänst för att upptäcka, förebygga och avvärja säkerhetshotande verksamhet som riktas mot Försvarsmakten och dess säkerhetsintressen.

Enligt *punkten 1* får uppgifter behandlas för att klarlägga verksamhet som innefattar hot mot rikets säkerhet. Därvid får under de närmare förutsättningar som anges i 9 § också behandlas uppgifter om personer med anknytning till sådan verksamhet. Med denna punkt avses säkerhetsunderrättelsetjänst. Verksamhet sker i stort under samma arbetsformer och med utnyttjande av samma typ av källor som används i försvarsunderrättelseverksamheten.

Inom säkerhetskyddstjänsten, som avses i *punkten 2*, vidtas olika åtgärder för att förhindra eller försvåra säkerhetshotande verksamhet. Härvid arbetar man med att förebygga att hemliga uppgifter som rör rikets säkerhet obehörigen röjs, ändras eller förstörs. Verksamheten syftar också till att skydda Försvarsmaktens personal, materiel och anläggningar.

I säkerhetskyddstjänsten innefattas signalskyddstjänsten. Punkten 2 omfattar följaktligen också signalskyddstjänst, som syftar till att minska verkan av signalspaning, falsk signalering och störsändning mot totalförsvarets telekommunikations- och informationssystem. Verksamheten skall förhindra obehörig insyn i och påverkan av totalförsvarets telekommunikationer, samt användning av kryptografiska funktioner i informationssystemen. Signalkontroll innebär att underlag inhämtas främst genom avlyssning av analog och digital signalering i telekommunikations- och informationssystem. De inhämtade underlagen granskas och bearbetas, varefter gjorda iakttagelser delges och rapporteras. Signalkontroll genomförs i totalförsvarets telekommunikations- och informationssystem stickprovvis med hjälp av fasta eller rörliga kontrollorgan. I 10 §

återfinns en särskild bestämmelse om personuppgiftsbehandling i signalkontrollverksamheten.

9 §

I paragrafen preciseras de ändamål för vilka personuppgifter får behandlas inom den militära säkerhetstjänsten med en särskild bestämmelse om vilka uppgiftskategorier som får behandlas i verksamheten. Av *första stycket* framgår att uppgifter om en person i huvudsak får behandlas endast om uppgifterna ger grundad anledning anta att personen utövat eller kan komma att utöva säkerhetshotande verksamhet eller har lämnat uppgift om sådan verksamhet samt om uppgifterna har framkommit genom att någon genomgått säkerhetsprövning enligt säkerhetsskyddslagen (1996:627). Punkten 1 omfattar verksamhet som innefattar sådant hot mot rikets säkerhet som utgör brott eller terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott. Nämda lag trädde i kraft den 1 juli 2003 och det finns ett behov av att behandla uppgifter om personer som kan antas ha utövat motsvarande verksamhet dessförinnan. Därför anges att den verksamhet som kan läggas till grund för personuppgiftsbehandling även omfattar motsvarande brottslighet enligt tidigare lagstiftning, d.v.s. sådant våld, hot eller tvång för politiska syften som i 14 § första stycket 1 förordningen (2001:703) om viss behandling av personuppgifter inom Försvarmakten och Försvarets radioanstalt betecknas som terrorism. I punkterna 2 och 3 anges vilken säkerhetshotande verksamhet i övrigt som kan läggas till grund för personuppgiftsbehandling.

När uppgifter behandlas i den militära säkerhetstjänsten är det av integritetsskäl viktigt att man särskiljer olika typer av uppgifter. Särskilt viktigt är att det inte uppstår missuppfattningar om i fall någon kan antas faktiskt utöva eller förbereda säkerhetshotande verksamhet eller inte. I *andra stycket* anges att uppgifter om en person skall förse med upplysning om på vilken av de i första stycket angivna grunderna uppgiften behandlas. Uppgifter om brottsmisstanke är särskilt känsliga ur

integritetssynpunkt och det föreskrivs därför att i de fall behandlingen av en personuppgift inte föranleds av antagande om att personen utövar brottslig verksamhet skall detta särskilt anges, om det inte klart framgår på annat sätt. På motsvarande sätt skall anges om det inte heller kan antas att personen bedriver säkerhetshotande verksamhet som inte utgör brott. Utgångspunkten är dock att särskilda upplysningar inte behövs när det av sammanhanget inte kan uppstå några tvivel om varför uppgifterna i fråga behandlas och det därför inte föreligger risk för att någon av misstag kan uppfattas utöva brottslig eller på annat sätt säkerhetshotande verksamhet.

I tredje stycket föreskrivs att uppgifter om att en person som avses i punkterna 1 och 2 skall förses med upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. Detta innebär att en särskild upplysning i förekommande fall skall lämnas om vilken trovärdighet som tillmäts t.ex. den som lämnat ett tips till säkerhetstjänsten. Om möjligt skall också anges hur korrekt uppgiften är, t.ex. om det är en obekräftad gissning eller ett belagt faktum.

10 §

Bestämmelsen innebär att personuppgifter som ingår i eller har uppkommit i samband med användning av totalförsvarets telekommunikations- och informationssystem – även sådana som omfattas av särskilda restriktioner – får behandlas i syfte att förhindra obehörig insyn i och påverkan av dessa system. Den omständigheten att sådan behandling genom signalkontroll utförs utan att förekomsten av relevanta personuppgifter på förhand kan avgöras utgör följaktligen inte något hinder för verksamheten.

När säkerhetshotande företeelser upptäcks och det erfordras särskild behandling för att identifiera en person, t.ex. genom att en viss kommunikationsenhet härleds till en individualiserad användare, gäller dock att behandlingen endast får utföras om det finns grundad anledning att anta att det beträffande personen föreligger sådant förhållande som avses i 9 §

första stycket 1, 2 eller 3.

Av *andra stycket* framgår att när en behandling utförs i det specifika syftet att identifiera en person skall denna behandling upptas i en förteckning som också skall innehålla de uppgifter som utgjort anledningen till behandlingen. Denna reglering möjliggör kontroll av att sådana behandlingar – vilka får anses känsliga ur integritetssynpunkt – endast företas när tillräckliga skäl föreligger.

Behandling av känsliga personuppgifter

11 §

I *första stycket* anges att känsliga personuppgifter inte får behandlas enbart på grund av vad som är känt om personens ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexualliv. Det innebär t.ex. att det inte är tillåtet att föra register över, eller på annat sätt göra anteckningar om, enskilda personer enbart på den grunden att de tillhör en viss etnisk grupp.

Av *andra stycket* framgår att om uppgifter om en person behandlas på annan grund får de kompletteras med känsliga personuppgifter när det är oundgängligen nödvändigt för syftet med behandlingen. Uppgifter som beskriver en persons utseende skall alltid utformas på ett objektiva sätt med respekt för människovärdet.

I den verksamhet som regleras i lagen är uppgifter om etniskt ursprung, politiska åsikter och religiös övertygelse sådana faktorer som är av stor betydelse när det gäller att bedöma personers eller grupperns agerande i ett ur försvarsunderrättelseperspektiv relevant avseende. Inte minst gäller detta vid försvarsunderrättelseverksamhet till stöd för svenska militära operationer utomlands, då konflikterna ofta har sitt ursprung i etniska, politiska eller religiösa motsättningar. I sådana fall får behandling av känsliga personuppgifter anses oundgängligen nödvändig för syftet med behandlingen.

Om Försvarsmakten i den militära säkerhetstjänsten får ett

tips om att en viss person kan komma att bedriva säkerhetshotande verksamhet av något slag får naturligtvis anteckningar göras om det är nödvändigt för att möjliggöra identifiering av denna person, t.ex. uppgifter om fysiska kännetecken eller etniskt ursprung m.m.

Det *tredje styckte* reglerar under vilka förutsättningar känsliga uppgifter får användas som sökbegrepp. Bestämmelsen är tillämplig oavsett om sökning sker i en uppgiftssamling eller i annat material. Bestämmelserna utesluter inte att känsliga personuppgifter kan användas ensamma vid sökning. Det är således inte nödvändigt att vid användning av en känslig personuppgift som sökbegrepp alltid använda ett kompletterande sökord som inte utgör en känslig personuppgift. De känsliga personuppgifterna får dock inte utgöra det enda ändamålet med sökningen. Också här uppställs kravet att användningen av känsliga uppgifter skall vara oundgängligen nödvändig för syftet med behandlingen.

Behandling av personnummer

12 §

Bestämmelsen motsvarar 22 § personuppgiftslagen med undantag av att samtycke från den enskilde inte tillåter behandling av personnummer eller samordningsnummer i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst, se avsnitt 8.8.

Utlämnande av personuppgifter på medium för automatiserad behandling

13 §

Paragrafen reglerar under vilka förutsättningar uppgifter får lämnas ut i elektronisk form, t.ex. i ett e-postmeddelande eller på diskett. Bestämmelsen har inte någon sekretessbrytande verkan.

Bestämmelsen innebär att en större mängd personuppgifter, t.ex. ett helt register eller delar av ett register, inte får lämnas ut på medium för automatiserad behandling utan att regeringen har meddelat föreskrifter eller beslut om detta. Däremot kan enstaka uppgifter lämnas ut. När personuppgifter förekommer i en eller ett fåtal handlingar utgör bestämmelsen inte något hinder mot att lämna ut handlingarna genom t.ex. ett e-postmeddelande, även om handlingen eller handlingarna i och för sig innehåller något fler personuppgifter än vad som i vanligt språkbruk avses med enstaka.

Direktåtkomst

14 §

Bestämmelsen innebär att regeringen har möjlighet att föreskriva eller besluta om att annan myndighet får ha direktåtkomst till personuppgifter. Om en sådan åtkomstmöjlighet ges skall omfattningen av direktåtkomsten regleras av regeringen eller den myndighet regeringen bestämmer. Se vidare avsnitt 8.21.3.

Tillgången till personuppgifter

15 §

Med hänsyn till skyddet för den personliga integriteten skall personuppgifter inte spridas till en vidare krets inom Försvarsmakten än nödvändigt. I paragrafen föreskrivs därför att tillgången till personuppgifter skall vara förbehållen de personer som behöver tillgång till uppgifterna för att kunna fullgöra sina arbetsuppgifter. Av verksamhetens art följer att inskränkningar av behörigheten också är nödvändiga av säkerhetsskäl.

Överföring av personuppgifter till andra länder

16 §

Enligt *första stycket* får personuppgifter föras över ut till andra länder om sekretess inte hindrar det och det är nödvändigt för att Försvarsmakten skall kunna fullgöra sina uppgifter inom ramen för det internationella försvarsunderrättelse- och säkerhetssamarbetet. Paragrafen är ägnad att uppfylla de krav på nationell lagstiftning som dataskyddskonventionen ställer när det gäller överföring av personuppgifter till andra länder. Huruvida ett utlämnade skall ske eller inte måste i sin helhet avgöras efter en sekretessprövning och försvars- och säkerhetspolitiska överväganden.

I *andra stycket* bemyndigas regeringen att föreskriva eller i särskilt fall besluta att överföring även får ske i andra fall än inom ramen för det internationella försvarsunderrättelse- och säkerhetssamarbetet om det är nödvändigt för att Försvarsmakten skall kunna fullgöra sina uppgifter. Det kan t.ex. vid ett förband i utlandsstyrkan inom Försvarsmakten i vissa situationer vara nödvändigt att överlämna underrättelser till ett organ i en annan stats väpnade styrkor som inte kan sägas vara ett underrättelse- eller säkerhetsorgan.

Uppgiftssamlingar

17 §

I paragrafen anges att det får finnas ett antal skilda samlingar uppgifter som med hjälp av automatiserad behandling används gemensamt i respektive verksamhet. Uppgifterna har hämtats in i den militära underrättelse- och säkerhetstjänsten och har gjorts gemensamt tillgängliga för olika handläggare inom organisationen med den begränsning som följer av befattningshavarens behörighet. Utanför uppgiftssamlingarna faller däremot uppgifter i t.ex. e-post, ordbehandlingsdokument och

tillfällig behandling av uppgifter som lagras på en hårddisk eller i en server på sådant sätt att de inte är allmänt tillgängliga inom Försvarsmakten, utan åtkomliga endast för den person – eller ett fåtal personer i en begränsad grupp – som tar emot e-postmeddelandet, upprättar dokumentet eller använder sig av de tillfälligt behandlade uppgifterna m.m.

I paragrafens *andra stycke* bemyndigas regeringen att meddela närmare föreskrifter eller beslut om vilka uppgifter som får behandlas i databaserna. De i 9 § angivna bestämmelserna om uppgifter som behandlas i den militära säkerhetstjänsten gäller även för den behandling som sker i Försvarsmaktens uppgiftssamlingar.

2 kap. Information till den enskilde, rättelse och skadestånd

Information till den enskilde

Information som skall lämnas självmant

1 §

Bestämmelsen motsvarar 23 och 25 §§ personuppgiftslagen. För en kommentar se prop. 1997/98:44 s. 130 f.

Se avsnitt 8.11.

Information som skall lämnas efter ansökan

2 §

Bestämmelsen motsvarar 26 § första och andra stycket personuppgiftslagen. För en kommentar se vidare prop. 1997/98:44 s. 131 f.

Se avsnitt 8.11.

3 §

Bestämmelsen i *första stycket* innebär att information inte behöver lämnas i den utsträckning detta visar sig vara omöjligt eller skulle innebära en oproportionerligt stor arbetsinsats. Bestämmelsen överensstämmer med ett förslag lämnat av Per-

sonuppgiftslagsutredningen i bet. SOU 2004:6. I författningskommentaren till bestämmelsen har utredningen anfört följande.

Att information inte behöver lämnas om det visar sig vara omöjligt torde inte i sak innebära någon förändring av vad som gäller i dag.

Vad som skulle innebära en oproportionerligt stor arbetsinsats får bedömas i det enskilda fallet med beaktande av samtliga omständigheter. Om en personuppgiftsansvarig i motsvarande fall tidigare faktiskt lämnat registerutdrag enligt datalagen eller den hittillsvarande bestämmelsen i personuppgiftslagen, kan det i normalfallet inte anses vara fråga om en oproportionerligt stor arbetsinsats enligt den nya bestämmelsen. Syftet med ändringen är nämligen inte att inskränka det som faktiskt tillämpas i dag. Utredningen har således inte fått kännedom om något fall där ett registerutdrag faktiskt lämnats efter en oproportionerligt stor arbetsinsats.

Arbetsinsatserna kan gälla insatser för att finna alla uppgifter om den sökande som behandlas. Det kan ha särskild betydelse för en personuppgiftsansvarig som har en större mängd ostrukturerat material, t.ex. i form av löpande text eller ljud- och bildupptagningar, i synnerhet om materialet finns på olika ställen, t.ex. i hundratals persondatorer. Men det kan också gälla en personuppgiftsansvarig som har väldigt många regelrätta register att söka igenom. Det får göras en bedömning från fall till fall vilken arbetsinsats som är proportionerlig. Att personuppgifterna är kodade eller krypterade innebär inte i sig att det skulle innebära en oproportionerligt stor arbetsinsats att lämna information.

I de allra flesta fall måste det krävas att den personuppgiftsansvarige frågar den sökande efter sådana upplysningar som kan underlätta sökandet efter personuppgifterna. Lämnar den sökande användbara sådana upplysningar, måste det som regel krävas att den personuppgiftsansvarige åtminstone använder sig av upplysningarna för att söka efter uppgifterna. Om den personuppgiftsansvarige å andra sidan inte får efterfrågade upplysningar från den sökande, ligger det närmare till hands att anse att ett

förutsättningslöst sökande innebär en oproportionerligt stor arbetsinsats i förhållande till det intresse sökanden visat. I de fall där den sökande kan göra troligt att en annan person använt sökandens identitet vid kontakter med den personuppgiftsansvarige, kan den sökande ibland inte lämna konkreta upplysningar om var de felaktiga personuppgifterna kan finnas. Men det är i detta fall ändå oftast befogat att den personuppgiftsansvarige lägger ned en ganska stor arbetsinsats för att finna alla aktuella personuppgifter av betydelse.

Arbetsinsatsen kan också gälla insatser för att lämna information skriftligt till den registrerade. Det kan ha särskild betydelse i fråga om ljud- och bildupptagningar. Om det skulle innebära en oproportionerligt stor arbetsinsats att lämna informationen skriftligt, bör den registrerade åtminstone beredas tillfälle att få ta del av informationen på annat sätt, t.ex. vid besök på plats. Skyldigheten att lämna information bortfaller nämligen bara i den utsträckning den skulle innebära en oproportionerligt stor arbetsinsats.

Andra stycket motsvarar i princip 26 § tredje stycket personuppgiftslagen. För en kommentar se prop. 1997/98:44 s. 131.

Se avsnitt 8.11.

Undantag från informationskyldigheten vid sekretess

4 §

Bestämmelsen motsvarar till sin innebörd 27 § första meningen personuppgiftslagen. För en kommentar se prop. 1997/98:44 s. 133.

Se avsnitt 8.11.

Rättelse

5 §

Bestämmelsen motsvarar 28 § personuppgiftslagen, se vidare prop. 1997/98:44 s. 133 f.

Se avsnitt 8.12.

Skadestånd

6 §

Bestämmelsen motsvarar 48 § personuppgiftslagen, se vidare prop. 1997/98:44 s. 143 f.

Se avsnitt 8.13.

3 kap. Säkerheten vid behandling

1 §

Bestämmelsens första och andra stycke motsvarar 30 § första och andra stycket personuppgiftslagen, se vidare prop. 1997/98:44 s. 136.

Av 30 § tredje stycket personuppgiftslagen framgår att om det i lag eller annan författning finns särskilda bestämmelser om behandlingen av personuppgifter i det allmännas verksamhet i frågor som avses i första stycket skall dessa gälla i stället för vad som sägs i första stycket. Härmed avses enligt författningskommentaren (prop. 1997/98:44 s. 136) särskilt bestämmelser om tystnadsplikt och sekretess. I förslaget föreskrivs därför uttryckligen i paragrafens tredje stycke att i fråga om sekretess och tystnadsplikt i det allmännas verksamhet tillämpas bestämmelserna i sekretesslagen (1980:100) i stället för vad som föreskrivs i första stycket.

Se även avsnitt 8.14.

2 §

Bestämmelsen motsvarar 31 § personuppgiftslagen, se vidare prop. 1997/98:44 s. 136.

Se avsnitt 8.14.

4 kap. Personuppgiftsombud

1 §

I paragrafen föreskrivs att Försvarsmakten skall utse ett eller flera personuppgiftsombud. Myndigheten har således, till skillnad från vad som gäller enligt personuppgiftslagen, inte någon valfrihet härvidlag. Ett personuppgiftsombud skall anmälas till tillsynsmyndigheten såväl när det utses som när det entledigas.

2-4 §§

Bestämmelserna motsvarar i huvudsak 38–40 §§ personuppgiftslagen, se vidare prop. 1997/98:44 s. 139–141.

3 § har med hänsyn till att personuppgiftsombud alltid skall finnas formulerats något annorlunda än 39 § personuppgiftslagen. Separata förteckningar skall föras över automatiserade behandlingar av personuppgifter i försvarsunderrättelseverksamheten respektive den militära säkerhetstjänsten. Vad förteckningarna skall innehålla föreskrivs av regeringen eller den myndighet regeringen bestämmer.

5. kap Tillsynsmyndigheten

1 §

I förordning i anslutning till lagen skall anges att Datainspektionen är den myndighet som, i likhet med vad som nu gäller, skall utöva tillsyn över Försvarsmaktens behandling av personuppgifter.

2 §

Bestämmelsen motsvarar 43 § personuppgiftslagen, se vidare prop. 1997/98:44 s. 142.

3 §

Bestämmelsen motsvarar 45 § första stycket 1 personuppgiftslagen, se vidare prop. 1997/98:44 s. 142. Till skillnad från vad som gäller enligt personuppgiftslagen ges tillsynsmyndigheten här inte möjlighet att vid vite förbjuda fortsatt personuppgiftsbehandling, eftersom vite inte kan anses utgöra en lämplig sanktion i förhållandet mellan myndigheter, se vidare avsnitt 8.17.

4 §

Bestämmelsen motsvarar 47 § personuppgiftslagen, se vidare prop. 1997/98:44 s. 142 f. I paragrafen anges uttryckligen att den länsrätt vid vilken ansökan skall ske är länsrätten i Stockholms län.

6 kap. Övriga bestämmelser

Gallring

1 §

I paragrafen anges i vilken utsträckning personuppgifter som behandlas automatiserat skall gallras. Traditionellt sett har gallring inneburit utsortering och förstöring av dokument. I samband med gallringen har alltså såväl informationen som informationsbäraren försvunnit. I fråga om information på ADB-medier anses dock att gallring sker även då den elektroniskt lagrade informationen överförs till en pappersutskrift och sedan raderas från ADB-mediet. Avgörande för om gallring skall anses ha skett är om olika möjligheter att söka i eller göra sammanställningar av materialet gått förlorade (SOU 2002:97 s. 73). Riksarkivet har i sina föreskrifter (RA-FS 1991:1 och 1994:2) definierat gallring enligt följande.

Gallra: förstöra allmänna handlingar eller uppgifter i allmänna handlingar; förstöring av sådana handlingar/uppgifter i samband med överföring till annan databärare räknas som gallring om överföringen medför

- informationsförlust,
- förlust av möjliga informationssammanställningar,
- förlust av sökmöjligheter eller
- förlust av möjligheter att fastställa informationens autenticitet.

I paragrafen används begreppet gallring enligt den ovan angivna definitionen.

Som huvudregel skall gallring av automatiskt behandlade personuppgifter ske så snart uppgifterna inte längre behövs för det ändamål för vilket de behandlas. Uppgifter som lagras i pappersbaserade system omfattas inte av gallringsbestämmelsen. För dessa gäller istället arkivlagens (1190:782) bestämmelser. Huvudregeln innebär att myndigheten kontinuerligt skall pröva om personuppgifter behövs för verksamhetens ändamål. Kontrollen av att så sker äger rum inom ramen för den särskilda granskning som beskrivs i avsnitt 8.16.

I fråga om vissa uppgifter kan det finnas skäl att i stället för huvudregeln ange bestämda gallringsfrister. Regeringen beordras därför att meddela föreskrifter om att gallring skall ske senast vid viss tidpunkt.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om att personuppgifter utan hinder av den allmänna gallringsbestämmelsen får bevaras för historiska, statistiska och vetenskapliga ändamål.

Se vidare avsnitt 8.20.

Straff

2 §

Bestämmelsen motsvarar till viss del 49 § personuppgiftslagen, se vidare prop. 1997/98:44 s. 145 f. Eftersom det inte föreskrivs någon anmälningsskyldighet motsvarande 36 eller 41 § personuppgiftslagen anges dock inte bland straffbara förfaranden underlåtenhet att göra sådan anmälan, jfr 49 § första stycket i personuppgiftslagen. Bestämmelsen i 1 kap. 16 § om överföring till andra länder har inte formulerats som ett förbud mot överföring till vissa länder, varför inte 49 § första

stycket c har någon motsvarighet i paragrafen. Någon möjlighet för tillsynsmyndigheten att vid vite förbjuda viss behandling av personuppgifter föreslås inte i lagen, varför paragrafen inte heller innehåller någon reglering motsvarande 49 § tredje stycket personuppgiftslagen.

En ytterligare skillnad i förhållande till personuppgiftslagens nuvarande reglering ligger i att det i enlighet med Personuppgiftslagsutredningens förslag (SOU 2004:6 s. 201–203 och 278) krävs uppsåt eller grov oaktsamhet för att straffrättsligt ansvar skall ifrågakomma. Se vidare avsnitt 8.18.

Överklagande

3 §

Lagen ger inte tillsynsmyndigheten sådana befogenheter att någon bestämmelse om överklagande av tillsynsmyndighetens beslut är nödvändig (jfr 51 § personuppgiftslagen). Däremot kan Försvarsmakten med stöd av lagen komma att meddela beslut som rör enskilda, framförallt beslut om information respektive rättelse. Sådana beslut är överklagbara. Talan mot beslut om information och rättelse förs i den normalt gällande ordningen i fråga om förvaltningsbeslut, nämligen till allmän förvaltningsdomstol, d.v.s. länsrätt. Vid överklagande till kamrarrätten krävs prövningstillstånd.

12.2 Förslag till lag om behandling av personuppgifter i Försvarets radioanstalts underrättelseverksamhet

1 kap. Allmänna bestämmelser

Lagens tillämpningsområde m.m.

1 §

I *första stycket* anges lagens tillämpningsområde. Lagen är tillämplig vid behandling av personuppgifter i Försvarets radioanstalts underrättelse- och utvecklingsverksamhet, 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 som är tillgänglig för sökning eller sammanställning enligt särskilda kriterier. Med personuppgifter avses detsamma som i personuppgiftslagen, nämligen all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet. Behandling av uppgifter om avlidna personer och juridiska personer omfattas inte av lagen. Vad som avses med underrättelse- och utvecklingsverksamhet definieras inte i lagen, men ledning kan hämtas från ändamålsbestämmelserna, se avsnitt 8.5. För behandling av personuppgifter i den interna verksamheten gäller personuppgiftslagen (1998:204). Se även avsnitt 7.3 vad gäller tillämpningsområdet.

Bestämmelserna i 1 kap. är generella och gäller, om inte annat sägs, för all behandling av uppgifter i Försvarets radioanstalts underrättelseverksamhet, oavsett om det gäller e-post, enskilda tjänstemäns promemorior som upprättas i ordbehandlingsprogram, mindre register som används tillfälligt i underrättelseprojekt eller större register och datorsystem som används gemensamt i verksamheterna.

För tydlighetens skull anges i *andra stycket* lagens förhållan-

de till personuppgiftslagen. Den föreslagna lagen är heltäckande och innehåller alltså alla de bestämmelser som skall vara tillämpliga vid Försvarets radioanstalts behandling av personuppgifter i underrättelse- och utvecklingsverksamheten. Personuppgiftslagen gäller följaktligen inte vid sådan behandling. De närmare övervägandena framgår av avsnitt 7.2.

2 §

Bestämmelsen motsvarar 1 kap 2 § i förslaget till lag om behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst. För en kommentar hänvisas till den bestämmelsen.

Förhållandet till offentlighetsprincipen

3 §

Bestämmelsen motsvarar 1 kap 3 § i förslaget till lag om behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst. För en kommentar hänvisas till den bestämmelsen.

Definitioner

4 §

Bestämmelsen motsvarar 1 kap 4 § i förslaget till lag om behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst. För en kommentar hänvisas till den bestämmelsen.

Personuppgiftsansvar

5 §

Bestämmelsen motsvarar 1 kap 5 § i förslaget till lag om behandling av personuppgifter i Försvarmaktens försvarsunder-

rättelseverksamhet och militära säkerhetstjänst. För en kommentar hänvisas till den bestämmelsen.

Grundläggande krav på behandling av personuppgifter

6 §

Bestämmelsen motsvarar 1 kap 6 § i förslaget till lag om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst. För en kommentar hänvisas till den bestämmelsen.

När behandling av personuppgifter är tillåten

Underrättelseverksamhet

7 §

Paragrafen anger de ändamål för vilka uppgifter får användas – dvs. samlas in, registreras, lämnas ut och i övrigt behandlas – i Försvarets radioanstalts underrättelseverksamhet genom en hänvisning till lagen (2000:130) om försvarsunderrättelseverksamhet. Ändamålet omfattar därmed också de förändringar som föreslås i Ds 2005:30, se vidare avsnitt 6. Försvarets radioanstalts underrättelseverksamhet bedrivs genom signalspanning.

Försvarsunderrättelseverksamheten skall identifiera och redovisa eller ge förvarning om sådana förändringar i omvärldsläget att detta kan ligga till grund för politiska beslut om totalförsvarets anpassning på kort eller lång sikt. Totalförsvaret är den verksamhet som behövs för att förbereda Sverige för krig och består av militär verksamhet (militärt försvar) och civil verksamhet (civilt försvar), se 1 § lagen (1992:1403) om totalförsvaret och höjd beredskap.

Uppgifter behandlas vid Sveriges deltagande vid internationella fredsbevarande och humanitära insatser, samt för att stärka samhällets förmåga att förebygga och hantera svåra på-

frestningar på samhället. Det gäller att kunna förutse konflikter samt bearbeta inhämtat material och delge bedömningar om säkerhetspolitiska och militära förhållanden. Det kan också röra sig om att medverka med information och analys i fråga om sådant som t.ex. internationell terrorism och gränsöverskridande miljöhot.

Personlig information om t.ex. militär personal, politiker eller andra viktiga befattningshavare behandlas. Sådana uppgifter är nödvändiga att behandla för att informationsunderlaget till stöd för svensk utrikes-, försvars- och säkerhetspolitik skall bli komplett.

Andra stycket motsvarar 1 kap 7 § andra stycket i förslaget till lag om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst. För en kommentar hänvisas till den bestämmelsen

8 §

Paragrafen anger de ändamål för vilka personuppgifter får behandlas hos Försvarets radioanstalt i den underrättelseverksamhet som inte utgör försvarsunderrättelseverksamhet. Ändamålen korresponderar delvis med 2 § förordningen (1994:714) med instruktion för Försvarets radioanstalt samt med de ändamål utöver försvarsunderrättelseverksamheten för vilka Försvarets radioanstalt enligt förslaget till lag om signalspaning (Ds 2005:30) skall få inhämta signaler i elektronisk form. Av paragrafen framgår att verksamheten skall bedrivas i enlighet med vad regeringen bestämmer.

Utvecklingsverksamhet

9 §

Försvarets radioanstalt har enligt 3 § förordningen (1994:714) med instruktion för Försvarets radioanstalt till uppgift att, utöver underrättelseverksamheten, också bedriva viss utvecklingsverksamhet. I den huvudsakligen tekniskt inriktade verksamheten med att biträda andra myndigheter vid värdering,

utveckling, anskaffning och drift av signalspaningssystem används autentiskt underrättelsematerial – som kan innehålla personuppgifter – för att kontrollera systemens funktion. I paragrafen anges därför att behandling av personuppgifter skall få ske även för detta ändamål. Paragrafen innehåller också ett uttryckligt förbud att använda sådana uppgifter för andra ändamål eller lämna ut dem till annan. Se vidare avsnitt 8.5.

Behandling av känsliga personuppgifter

10 §

Bestämmelsen motsvarar 1 kap 11 § i förslaget till lag om behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst. För en kommentar hänvisas till den bestämmelsen.

Behandling av personnummer

11 §

Bestämmelsen motsvarar 1 kap 12 § i förslaget till lag om behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst. För en kommentar hänvisas till den bestämmelsen.

Utlämnande av personuppgifter på medium för automatiserad behandling

12 §

Bestämmelsen motsvarar 1 kap 13 § i förslaget till lag om behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst. För en kommentar hänvisas till den bestämmelsen.

Direktåtkomst

13 §

Bestämmelsen motsvarar 1 kap 14 § i förslaget till lag om behandling av personuppgifter i Försvarmaktens försvarsunder rättelseverksamhet och militära säkerhetstjänst. För en kommentar hänvisas till den bestämmelsen.

Tillgången till personuppgifter

14 §

Bestämmelsen motsvarar 1 kap 15 § i förslaget till lag om behandling av personuppgifter i Försvarmaktens försvarsunder rättelseverksamhet och militära säkerhetstjänst. För en kommentar hänvisas till den bestämmelsen.

Behandling av personuppgifter i vissa fall

15 §

Innan den information som Försvarets radioanstalt inhämtar genom signalspaning har bearbetats finns inte förutsättningar för att bedöma om den innehåller personuppgifter (se vidare avsnitt 8.9). Den initiala behandling som krävs för att detta skall kunna klarläggas måste kunna äga rum utan hinder av bestämmelserna i 6–11 §§. I paragrafen anges därför att Försvarets radioanstalts behandling av personuppgifter som innebär inhämtning av personuppgifter genom signalspaning, lagring av uppgifter som sker omedelbart därefter och bearbetning i form av kryptoforcering och språklig översättning inte skall anses som oförenlig med bestämmelserna om grundläggande krav, ändamål samt behandling av känsliga personuppgifter och personnummer. Så snart det kunnat fastställas om den inhämtade, lagrade eller bearbetade informationen inne-

håller personuppgifter måste dock vidare behandling av sådana personuppgifter som förekommer i materialet ske i överensstämmelse med 6–11 §§.

Överföring av personuppgifter till andra länder

16 §

Bestämmelsen motsvarar 1 kap 16 § i förslaget till lag om behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst. För en kommentar hänvisas till den bestämmelsen.

Uppgiftssamlingar

17 §

Bestämmelsen motsvarar 1 kap. 17 § i förslaget till lag om behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst. För kommentarer hänvisas till dessa bestämmelser.

2 kap. Information till den enskilde, rättelse och skadestånd

1-5 §§

Bestämmelserna motsvarar 2 kap. 2-6 §§ i förslaget till lag om behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst. För kommentarer hänvisas till dessa bestämmelser.

3 kap. Säkerheten vid behandling

1-2 §§

Bestämmelserna motsvarar 3 kap. 1-2 §§ i förslaget till lag om behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst. För kom-

mentarer hänvisas till dessa bestämmelser.

4 kap. Personuppgiftsombud

1-4 §§

Bestämmelserna motsvarar 4 kap. 1-4 §§ i förslaget till lag om behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst. För kommentarer hänvisas till dessa bestämmelser.

5 kap. Tillsynsmyndigheten

1-4 §§

Bestämmelserna motsvarar 5 kap. 1-4 §§ i förslaget till lag om behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst. För kommentarer hänvisas till dessa bestämmelser.

6 kap. Övriga bestämmelser

1-3 §§

Bestämmelserna motsvarar 6 kap. 1-3 §§ i förslaget till lag om behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst. För kommentarer hänvisas till dessa bestämmelser.

Bilaga 1

Sammanfattning av Underrättelsesdatautredningens betänkande Försvarets underrättelseverksamhet och säkerhetstjänst Integritet – Effektivitet (SOU 2003:34)

Några allmänna utgångspunkter för uppdraget

Den 24 oktober 1998 trädde personuppgiftslagen (1998:204) i kraft. Genom lagen genomförde Sverige 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).

Vi har haft i uppdrag att göra en översyn av regleringen av behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet. Den närmare regleringen av behandlingen av personuppgifter inom dessa verksamheter finns i dag i förordningen (2001:703) om viss behandling av personuppgifter inom Försvarmakten och Försvarets radioanstalt. Syftet med vårt uppdrag har varit att kartlägga behandlingen av personuppgifter och analysera behovet av särskilda bestämmelser samt lämna förslag till reglering i lag. I uppdraget har ingått att granska frågor som rör användning, inhämtande, utlämnande, gallring och arkivering av personuppgifter samt till-

syn över behandlingen. Vår utgångspunkt för uppdraget har varit att myndigheternas verksamhet skall kunna bedrivas effektivt och med ett rationellt datorstöd samtidigt som nödvändig respekt visas för enskildas personliga integritet. Vi har även haft att beakta det internationella inslaget i myndigheternas verksamheter.

Övergripande principer för ny lagstiftning

Lag, förordning och myndighetsföreskrifter

Utvecklingen inom datorområdet visar att lagstiftning som reglerar användningen av datorstöd måste vara teknikneutral och flexibel, för att inte hindra den effektivisering av verksamheterna som kontinuerligt pågår. Samtidigt är det mycket viktigt att det i lagstiftningen tas hänsyn till de registrerades personliga integritet.

I den militära underrättelse- och säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet hanteras stora mängder information som många gånger kan vara av känslig natur för de inblandade personerna. Hos båda myndigheterna pågår ständigt en teknisk utveckling av datorsystemen med ökade möjligheter att behandla och söka i stora uppgiftsmängder, vilket kan medföra en ökad risk för att enskilda drabbas av oacceptabla intrång i den personliga sfären. Det är viktigt att inte hamna i en situation där den tekniska utvecklingen styr den rättsliga regleringen, eller där den rättsliga regleringen onödigt hämmar effektiviseringen. Det är därför nödvändigt med en lagstiftning som enbart tar sikte på principiellt viktiga frågor och så långt som möjligt lämnar detaljregleringen därhän. Att beakta i sammanhanget är också att de aktuella verksamheterna är av sådan art att det inte är möjligt att i lagform reglera dem i detalj. Vi föreslår därför att de grundläggande principerna för behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet skall regleras särskilt i lag, medan kom-

pletterande bestämmelser skall meddelas av regeringen eller den myndighet regeringen bestämmer.

För behandling av personuppgifter i myndigheternas administrativa verksamhet, t.ex. i arbetsgivarfrågor, anser vi det tillräckligt med personuppgiftslagens bestämmelser och föreslår därför ingen särskild reglering inom det området.

Integritet och effektivitet

Utgångspunkten för vårt uppdrag att reglera viss behandling av personuppgifter hos Försvarmakten och Försvarets radioanstalt har varit att myndigheternas verksamheter skall kunna bedrivas effektivt samtidigt som nödvändig respekt visas för enskildas personliga integritet. Vid denna avvägning mellan integritet och effektivitet är det enligt vår uppfattning två omständigheter som framstår som särskilt betydelsefulla. För det första är det de *ändamål* för vilka behandling av personuppgifter får ske och för det andra den *säkerhet och sekretess* som gäller i verksamheterna.

Försvarsunderrättelseverksamhet bedrivs dels för att kartlägga yttre militära hot mot landet, dels till stöd för svensk utrikes-, försvars- och säkerhetspolitik. Den militära säkerhetstjänsten har till uppgift att upptäcka, identifiera och möta säkerhetshot som riktas mot Försvarmakten och dess intressen. Verksamheterna utgör grundläggande och viktiga samhällsfunktioner av stor betydelse för Sveriges yttre säkerhet och för att stärka samhället vid svåra påfrestningar i fred. Vi anser därför att en lagstiftning om behandling av personuppgifter måste ge Försvarmakten och Försvarets radioanstalt möjlighet att bedriva de aktuella verksamheterna på ett ändamålsenligt och effektivt sätt, även om det av vissa personer kan uppfattas medföra ett visst intrång i den personliga integriteten.

Försvarsunderrättelseverksamhet och militär säkerhetstjänst är verksamheter som av naturliga skäl till stor del måste vara hemliga. Många uppgifter som hanteras är känsliga såväl med hänsyn till Sveriges förhållande till främmande makt som till skyddet för rikets säkerhet. Det är också viktigt att skydda upp-

giftslämnare och arbetsmetoder. Den omfattande sekretess som omgärdar verksamheterna medför emellertid att det i jämförelse med annan verksamhet är mindre risk för att personuppgifter sprids till utomstående. Härmed är det i motsvarande mån mindre risk för att uppgifterna skall behandlas i strid med gällande ändamål, vilket i sig utgör ett skydd för den personliga integriteten.

Grundläggande för våra författningsförslag är att vi i lag anger tydliga och konkreta ändamål för behandling av personuppgifter. Behandling av personuppgifter som sker uteslutande enligt dessa särskilt fastlagda ändamål medför enligt vår uppfattning – med beaktande av den sekretess och säkerhet i övrigt som gäller i verksamheterna – inte någon påtaglig risk för *otillbörligt* intrång i registrerades personliga integritet. Vissa användningar, såsom t.ex. behandling av känsliga personuppgifter och annans direktåtkomst till elektroniskt lagrad information måste emellertid regleras särskilt. För att motverka den brist på insyn som följer av reglerna om sekretess bör vidare ett oberoende organ få till särskild uppgift att granska behandlingen av personuppgifter, för att ytterligare tillförsäkra att otillbörligt intrång i registrerades personliga integritet inte sker.

Lagstiftningens systematik och tillämpningsområde m.m.

Vi föreslår att den i dag gällande förordningen (2001:703) om viss behandling av personuppgifter inom Försvarmakten och Försvarets radioanstalts skall ersättas av två nya lagar med tillhörande förordningar. Den ena lagen reglerar behandling av uppgifter i Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten, medan den andra omfattar behandling av uppgifter i Försvarets radioanstalts underrättelseverksamhet.

De nya lagarna har samma inbördes systematik och delas in i tre kapitel. I ett första kapitel finns allmänna bestämmelser som i princip är tillämpliga på all behandling av uppgifter som omfattas av lagen. Det andra kapitlet innehåller särskilda bestämmelser som endast gäller automatiserad behandling av uppgifter i ge-

mensamma databaser. I det avslutande kapitlet finns bestämmelser om enskildas rättigheter vid behandling av personuppgifter, nämligen om information, rättelse, skadestånd och överklagande samt bestämmelser om särskild granskning till skydd för registrerades personliga integritet.

Lagarna tillämpas vid behandling av personuppgifter som är helt eller delvis automatiserad. Även behandling av personuppgifter i vissa manuella register omfattas av lagarnas tillämpningsområde. Grundläggande bestämmelser i lagarna, t.ex. när det gäller ändamålen med och ansvaret för behandlingen, är tillämpliga även vid behandling av uppgifter om juridiska personer.

Lagarna gäller i stället för personuppgiftslagen, vars bestämmelser tillämpas på behandling av personuppgifter hos Försvarsmakten och Försvarets radioanstalt endast när det anges särskilt. De bestämmelser i personuppgiftslagen som är allmänt tillämpliga är de om definitioner, förhållandet till offentlighetsprincipen, grundläggande krav på behandling, säkerheten vid behandling, personuppgiftsombudets uppgifter samt tillsynsmyndighetens befogenheter och straff.

Försvarsmakten och Försvarets radioanstalt är personuppgiftsansvariga för den behandling som myndigheterna utför eller som det åligger dem att utföra.

Tillåtna ändamål för behandling av personuppgifter

Försvarsmaktens och Försvarets radioanstalts behandling av personuppgifter skall styras av särskilt angivna och tydliga ändamål, vilka skall framgå av lag.

Försvarsmakten får behandla personuppgifter för ändamålen försvarsunderrättelseverksamhet och militär säkerhetstjänst. Med *försvarsunderrättelseverksamhet* avses att inhämta, bearbeta och analysera samt delge information dels för att kartlägga yttre militära hot mot landet, dels till stöd för svensk utrikes-, försvars- och säkerhetspolitik. Uppgifter får behandlas för säkerhetspolitiska och militärstrategiska bedömningar, analys av pågående och bedömda framtida konflikter samt biografisk försvars-

underrättelseverksamhet. I den *militära säkerhetstjänsten* får uppgifter behandlas för att upptäcka, förebygga och avvärja säkerhetshotande verksamhet som riktas mot Försvarsmakten och dess intressen. I verksamheten ingår *att* klarlägga verksamhet som innefattar hot mot rikets säkerhet och personer med anknytning till sådan verksamhet, *att* vidta åtgärder som hindrar eller försvårar säkerhetshotande verksamhet och *att* förhindra obehörig insyn i och påverkan av totalförsvarets telekommunikations- och informationssystem. I den militära säkerhetstjänsten får uppgifter om en person behandlas endast om personen har samband med säkerhetshotande verksamhet. Sådana uppgifter skall också föras med upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. Är personen inte misstänkt för att ha utövat eller komma att utöva säkerhetshotande verksamhet får uppgifter om denne behandlas endast om det klart framgår att sådan misstanke inte föreligger.

Försvarets radioanstalt får behandla uppgifter för att bedriva försvarsunderrättelseverksamhet samt för att i övrigt utföra de uppgifter som enligt instruktionen åligger myndigheten i dess *underrättelseverksamhet*. Med försvarsunderrättelseverksamhet avses här detsamma som ovan beskrivits för Försvarsmakten. Försvarets radioanstalt bedriver emellertid inte enbart militärt inriktad underrättelseverksamhet utan har också andra uppgifter som regeringens civila inhämtningsorgan i utrikes- och säkerhetspolitiska frågor. Försvarets radioanstalt skall även med sin tekniska expertis lämna stöd för annan myndighetsverksamhet än sådan som rör yttre hot mot rikets säkerhet.

Behandling av känsliga personuppgifter

Uppgifter om en person får inte behandlas enbart på grund av vad som är känt om personens ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexualliv (känsliga personuppgifter). Om uppgifter om en person behandlas på annan grund får de

emellertid kompletteras med känsliga personuppgifter, när det är nödvändigt för syftet med behandlingen.

Vid sökning i Försvarmaktens och Försvarets radioanstalts databaser får känsliga personuppgifter inte användas som sökbegrepp om det inte är nödvändigt. Sökning får inte ske enbart med en känslig personuppgift som grund utan måste även stödjas av ett för verksamheten annat berättigat skäl, och skall dessutom föregås av ett noggrant övervägande huruvida användningen av personuppgifterna tillför något av värde för verksamheten.

Utlämnande av uppgifter

Det internationella samarbetet inom underrättelse- och säkerhetstjänsten är av mycket stor betydelse för Sverige. Av gällande lagstiftning och regeringens regleringsbrev framgår att för såväl Försvarmakten som Försvarets radioanstalt skall samarbete med andra länder och internationella organisationer vara en naturlig del av verksamheten. För att främja inter-nationellt samarbete inom underrättelse- och säkerhetstjänsten anser vi att uppgifter för vilka sekretess gäller bör få lämnas ut till en utländsk myndighet eller en internationell organisation om utlämnandet tjänar den svenska statsledningen och det svenska totalförsvaret samt om lämnade uppgifter inte är till skada för svenska intressen.

Enligt vår uppfattning behöver utlämnande av uppgifter på medium för automatiserad behandling inte regleras särskilt. Sådant utlämnande kan förekomma till annan svensk myndighet och till annan stat eller internationell organisation. För svenska myndigheter finns ofta särskilda registerförfattningar som reglerar behandlingen av personuppgifter. Utlämnande till andra länder och internationella organisationer omfattas av höga krav på säkerhet och sekretess som betingas av ändamålet för verksamheten. Någon särskild integritetsskyddande regel är därför enligt vår mening inte nödvändig i dessa sammanhang.

På grund av Sveriges anslutning till Europarådets dataskyddskonvention är det emellertid nödvändigt med särskilda bestämmelser vid utlämnande av personuppgifter till andra länder. Vi

föreslår därför att uppgifter som behandlas med stöd av de författningar vi föreslår får lämnas ut till andra länder om sekretess inte hindrar det och det behövs för att myndigheterna skall kunna fullgöra sina uppgifter inom ramen för det internationella försvarsunderrättelse- och säkerhetssamarbetet eller det annars är nödvändigt för verksamheten. Bestämmelsen innebär inte i sig någon begränsning av myndigheternas möjlighet att lämna ut uppgifter, utan detta får i sin helhet avgöras efter försvars- och säkerhetspolitiska överväganden.

Behandling av uppgifter i databaser

Hos myndigheter behandlas i dag personuppgifter med datorstöd på i huvudsak två principiellt och tekniskt skilda sätt. För det första används persondatorer på så sätt att endast ett fåtal personer kan ta del av informationen, t.ex. enskilda tjänstemän som upprättar promemorior och beslutsunderlag m.m. samt skickar och tar emot e-post. För det andra används i stor utsträckning allmänt åtkomliga dataregister i form av gemensamma system med information som behövs i myndighetens verksamhet. Den senare formen av datorstöd anser vi bör omgärdas av särskilda skyddsregler, eftersom integritetsriskerna ökar när stora mängder information behandlas gemensamt. Vi föreslår att sådan behandling skall samlas under det rättsliga begreppet databas. Det rättsliga begreppet databas kan omfatta flera mindre register, databaser eller datorsystem.

Olika regler skall således gälla för Försvarsmaktens respektive Försvarets radioanstalts behandling av uppgifter beroende på om behandlingen utförs av enskilda tjänstemän och uppgifterna inte görs tillgängliga för gemensam användning i verksamheten, eller om behandlingen är automatiserad och utförs i en särskild samling av uppgifter som används gemensamt i verksamheten (databaser).

Försvarets radioanstalts databaser

Försvarets radioanstalt bedriver underrättelseverksamhet genom att inhämta information dels via signalspaning dels från öppna källor. Försvarets radioanstalts system för behandling av personuppgifter i dess underrättelseverksamhet är helt anpassat till underrättelseprocessens led med planering och inriktning, inhämtning, bearbetning och analys samt delgivning. I enlighet härmed skall det för uppgifter som används vid planering och inriktning av myndighetens underrättelseverksamhet på kort och på lång sikt finnas en urvalsdatabas. Information som hämtas in genom signalspaning skall lagras i en källdatabas medan övrig information lagras i en databas för öppna källor. Bearbetning och analys av inhämtad underrättelseinformation skall ske i en analysdatabas och de underrättelserapporter som är färdiga för delgivning skall slutligen lagras i en rapportdatabas.

Försvarsmaktens databaser

Inom den militära underrättelse- och säkerhetstjänsten finns det i dag två typer av register eller databaser, antingen för öppen eller för hemlig information. Enligt den reglering av Försvarsmaktens databaser som vi föreslår skall det finnas en informationsdatabas samt en underrättelse- och säkerhetsdatabas. I informationsdatabasen får Försvarsmakten behandla information som inte är hemlig och som hämtats in från allmänt tillgängliga öppna källor.

Hemliga uppgifter lagras hos Försvarsmakten i flera olika datorbaserade system anpassade till ändamålet med den särskilda behandlingen. Den viktigaste databasen är härvid Informationssystem för den militära underrättelse- och säkerhetstjänsten (IS UNDSÄK). I databasen behandlas uppgifter som rör hela den militära underrättelse- och säkerhetstjänstens ansvarsområde. Det finns även vissa andra databaser för behandling av hemlig information med mer begränsade användningsområden, som t.ex. bearbetning och analys av uppgifter i samband med Sveriges deltagande i internationella operationer eller för kommunikation

med Sveriges försvarsattachéer. Underrättelse- och säkerhetsdatabasen är avsedd att vara ett samlande begrepp för de olika databaser i vilka Försvarsmakten behandlar hemliga uppgifter.

Innehåll

Det är inte möjligt att i detalj lagreglera vilka uppgifter som bör få behandlas i myndigheternas databaser. En noggrann reglering av vilka uppgifter som får behandlas måste även till viss del vara hemlig. Vi föreslår därför att regeringen eller den myndighet som regeringen bestämmer skall meddela närmare föreskrifter eller beslut om vilka uppgifter som får behandlas i Försvarsmaktens och Försvarets radioanstalts databaser. I förordning införs emellertid av upplysnings-skäl en bestämmelse om vilka uppgiftskategorier som får behandlas i databaserna. Även bestämmelserna om ändamål kan ge enskilda information om vilka uppgifter som registreras.

Direktåtkomst

Att tillåta direktåtkomst för myndigheter till information i andra myndigheters dataregister m.m. har länge ansetts särskilt integritetskänsligt. Vi delar den uppfattningen, men anser att det finns starka skäl för att tillåta sådan åtkomst. Vilka som får ha direktåtkomst till Försvarsmaktens och Försvarets radioanstalts databaser bestäms av regeringen i förordning eller beslut. Vi föreslår att direktåtkomst får förekomma mellan Försvarsmakten respektive Försvarets radioanstalt och i första hand Regeringskansliet. I viss utsträckning bör också de andra myndigheter som bedriver försvarsunderrättelseverksamhet eller i övrigt deltar i skyddet av rikets säkerhet ha direktåtkomst. Regeringen, eller den myndighet som regeringen bestämmer, bör meddela närmare föreskrifter eller beslut om omfattningen av direktåtkomsten.

Enskildas rättigheter

Fysiska personer bör av integritetsskäl ha vissa grundläggande rättigheter som rör behandlingen av uppgifter om dem. Förutom rätt till information, rättelse och skadestånd, anser vi att vissa beslut av Försvarsmakten och Försvarets radioanstalt bör kunna överklagas. Dessa rättigheter bör inte gälla för juridiska personer.

Således anser vi att personuppgiftslagens bestämmelser om information som skall lämnas självant till den registrerade när uppgifter samlas in från denne själv och om information som skall lämnas efter ansökan av den registrerade, i huvudsak bör tillämpas vid behandling av personuppgifter i de aktuella verksamheterna. Vidare bör personuppgiftslagens bestämmelser om rättelse av personuppgifter och om skadestånd tillämpas. Försvarsmaktens och Försvarets radioanstalts beslut om rättelse och om information som skall lämnas efter ansökan av en registrerad skall enligt vår mening kunna överklagas till allmän förvaltningsdomstol.

Särskild granskning till skydd för den personliga integriteten

Personuppgiftslagens regler om enskildas rätt till information är av stor betydelse för att personuppgifter inte skall behandlas på ett sätt som kan medföra att enskildas personliga integritet kränks. Den sekretess som gäller för uppgifter i de nu aktuella verksamheterna innebär emellertid att information i den mening som avses i personuppgiftslagen i praktiken aldrig kommer att lämnas av den personuppgiftsansvariga myndigheten. Av 27 § personuppgiftslagen följer nämligen att sekretess och tystnadsplikt alltid går före den i personuppgiftslagen föreskrivna informationsskyldigheten. Härigenom begränsas också de registrerades möjlighet att begära rättelse och skadestånd.

Det är enligt vår uppfattning nödvändigt att skyddet för registrerades personliga integritet kompletteras. Försvarets under rättelsenämnd bör därför få i uppdrag att särskilt granska den

behandling av personuppgifter som sker i Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet.

Försvarets underrättelsenämnd har till uppgift att följa underrättelsetjänsten inom Försvarmakten och de övriga myndigheter som bedriver försvarsunderrättelseverksamhet, bl.a. Försvarets radioanstalt. Härvid har nämnden redan i dag som särskild uppgift att granska hur de register som behövs för försvarsunderrättelseverksamhet läggs upp och förs. Försvarets underrättelsenämnd framstår med hänsyn härtill och till nämndens kunskaper om försvarsunderrättelseverksamhet som bäst lämpad att utföra granskning av behandlingen av personuppgifter enligt de författningar vi nu föreslår.

Förslaget om en särskild granskning syftar inte till att inskränka det övergripande tillsynsansvar som åligger Datainspektionen enligt personuppgiftslagen. Datainspektionen bör alltså ha huvudansvaret för tillsyn över behandlingen av personuppgifter hos Försvarmakten och Försvarets radioanstalt. Försvarets underrättelsenämnds granskning skall vara en extra integritetsskyddskontroll som, utöver Datainspektionens tillsyn, skyddar de registrerade mot kränkning av den personliga integriteten vid behandling av personuppgifter.

Försvarets underrättelsenämnd skall inte vara involverad i någon löpande ärendehantering hos de båda myndigheterna och enskilda skall inte kunna vända sig till nämnden med begäran om utlämnande av handlingar. En sådan begäran skall som i dag prövas av Försvarmakten eller Försvarets radioanstalt.

Bevarande och gallring

Registerförfattningar innehåller av integritetsskäl ofta bestämmelser som innebär att uppgifter som huvudregel inte får bevaras utan tidsgräns. I många sådana författningar finns därför bestämmelser om gallring av uppgifter eller om överlämnande av uppgifter till en arkivmyndighet. I nya registerförfattningar tillämpas vanligen en metod som innebär att det i lag ställs upp hu-

vudregler för när gallring av uppgifter skall ske, men med möjlighet för regeringen eller Riksarkivet att besluta eller meddela föreskrifter om att uppgifter skall bevaras.

När det gäller uppgifter i traditionella pappersbaserade allmänna handlingar är i stället huvudregeln att det inte finns några särbestämmelser utan arkivlagens regler gäller fullt ut. Det är också denna metod som vi anser bör gälla i fråga om bevarande och gallring av uppgifter i Försvarmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet.

I de aktuella verksamheterna måste uppgifter kunna sparas under mycket lång tid, ofta i minst 30 år och ibland så länge som upp till 70 år. Gallring syftar som nämnts i första hand till att värna skyddet för den personliga integriteten. Med hänsyn till bl.a. offentlighetsprincipen bör emellertid krav på gallring inte gälla som huvudregel utan att starkt vägande integritetsskäl talar härför. När uppgifter har bevarats i 30 år eller längre har enligt vår uppfattning integritetsintressena till stor del spelat ut sin roll. Gallring är vidare inte den enda metoden för att tillgodose skyddet för den personliga integriteten. Framför allt den sekretess som gäller i verksamheterna fungerar som ett starkt skydd för den personliga integriteten och talar mot nödvändigheten av att ha särskilda gallringsregler. Samtidigt tjänas integritetsintresset inte alltid bäst av att så många uppgifter som möjligt gallras. I vissa fall har bevarandet av känsliga uppgifter visat sig vara till stor fördel för enskilda. Vidare utgör offentlighetsintresset och den minskade möjligheten till insyn i myndigheternas verksamhet för bl.a. forskning skäl som talar mot omfattande gallring.

Mot bakgrund härav föreslår vi inte några särskilda gallringsbestämmelser för de aktuella verksamheterna. Det innebär att bestämmelserna i arkivlagen och personuppgiftslagen blir tillämpliga vad gäller frågor om bevarande och gallring, oavsett om uppgifterna behandlas i en databas eller inte. I praktiken innebär detta att allmänna handlingar som huvudregel skall bevaras och att handlingarna får gallras endast om Riksarkivet har tillåtit det. För andra uppgifter, dvs. sådana uppgifter som inte ingår i all-

männa handlingar, gäller i stället att de skall rensas (förstöras) när de inte längre behövs för de ursprungliga ändamålen med registreringen.

Sekretess till skydd för enskilds personliga eller ekonomiska förhållanden

I Försvarsmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten finns uppgifter som kan vara mycket integritetskänsliga för enskilda och deras närstående och som inte skyddas av gällande sekretessregler. Det kan t.ex. gälla uppgifter som avslöjar en persons fysiska eller psykiska hälsotillstånd. Den sekretess som i dag gäller för uppgifter i den militära underrättelse- och säkerhetstjänsten syftar endast till att skydda själva verksamheten hos myndigheten och utgör därmed inget skydd för enskilda individer och deras personliga eller ekonomiska intressen. Mot bakgrund härav föreslår vi att det i sekretesslagen (1980:100) införs en bestämmelse om sekretess hos Försvarsmakten i den militära underrättelse- och säkerhetstjänsten, till skydd för uppgift om enskilds personliga eller ekonomiska förhållanden. Sekretess för sådan uppgift skall enligt vår mening gälla om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon honom närstående lider skada eller men. Sekretess bör gälla i högst 70 år.

Bilaga 2

Underrättelsedatautredningens lagförslag

- 1 Förslag till lag om behandling av uppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten

Härigenom föreskrivs följande.

1 kap. Allmänna bestämmelser

Lagens tillämpningsområde m.m.

1 § Denna lag tillämpas vid behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten, om behandlingen är helt eller delvis automatiserad eller om uppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

Bestämmelserna i 4–6 §§ samt 2 kap. gäller även vid behandling av uppgifter om juridiska personer.

I 2 kap. finns särskilda bestämmelser om behandling av personuppgifter i den militära underrättelse- och säkerhetstjänstens databaser.

Förhållandet till personuppgiftslagen

2 § Om inte annat anges i 3 § eller i 3 kap. gäller denna lag i stället för personuppgiftslagen (1998:204).

3 § När personuppgifter behandlas enligt denna lag eller enligt andra föreskrifter i det ämne som regleras i lagen gäller personuppgiftslagens (1998:204) bestämmelser om

1. definitioner i 3 §,
2. förhållandet till offentlighetsprincipen m.m. i 8 §,
3. grundläggande krav på behandling i 9 §,
4. säkerheten vid behandling i 30 och 31 §§,
5. personuppgiftsombud m.m. i 36 § andra stycket och 38–40 §§,
6. tillsynsmyndighetens befogenheter i 43 och 47 §§, och
7. straff i 49 §.

Personuppgiftsansvar

4 § Försvarsmakten är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför eller som det åligger myndigheten att utföra. Motsvarande ansvar gäller för behandling av uppgifter om juridiska personer.

Ändamål m.m.

Försvarsunderrättelseverksamhet

5 § Uppgifter får behandlas i försvarsunderrättelseverksamheten dels för att kartlägga yttre militära hot mot landet dels till stöd

för svensk utrikes-, försvars- och säkerhetspolitik om det behövs för

1. säkerhetspolitiska och militärstrategiska bedömningar,
2. analyser av pågående och bedömda framtida konflikter, eller
3. biografisk försvarsunderrättelseverksamhet.

Militär säkerhetstjänst

6 § Uppgifter får behandlas i den militära säkerhetstjänsten för att upptäcka, förebygga och avvärja säkerhetshotande verksamhet som riktas mot Försvarsmakten och dess intressen om det behövs för

1. att klarlägga verksamhet som innefattar hot mot rikets säkerhet och personer med anknytning till sådan verksamhet (säkerhetsunderrättelsetjänst),
2. åtgärder som hindrar eller försvårar säkerhetshotande verksamhet (säkerhetsskyddstjänst), eller
3. att förhindra obehörig insyn i och påverkan av totalförsvarets tele-kommunikations- och informationssystem (signal-skyddstjänst).

7 § För de ändamål som anges i 6 § 1–2 får uppgifter om en person behandlas endast om

1. personen kan misstänkas för att ha utövat eller komma att utöva verksamhet som innefattar hot mot rikets säkerhet eller terrorism,
2. uppgifterna avser information som framkommit i samband med att en person har genomgått registerkontroll enligt säkerhetsskyddslagen (1996:627),
3. det kan antas att personen bedriver annan säkerhetshotande verksamhet än som avses i 1, och det finns särskilda skäl till att uppgiften skall behandlas, eller
4. personen har lämnat uppgifter om säkerhetshotande verksamhet.

Uppgifter om att en person kan antas ha samband med säkerhetshotande verksamhet skall förses med upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak.

Uppgifter om en person som inte misstänks för att ha utövat eller komma att utöva säkerhetshotande verksamhet får behandlas endast om det genom särskild upplysning eller på annat sätt klart framgår att sådan misstanke inte föreligger.

Behandling av känsliga personuppgifter

8 § Uppgifter om en person får inte behandlas enbart på grund av vad som är känt om personens ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexualliv.

Om uppgifter om en person behandlas på annan grund får de kompletteras med sådana uppgifter som avses i första stycket när det är nödvändigt för syftet med behandlingen.

Överföring av personuppgifter till tredje land

9 § Personuppgifter som behandlas med stöd av denna lag får lämnas ut till andra länder om sekretess inte hindrar det och det behövs för att Försvarsmakten skall kunna fullgöra sina uppgifter inom ramen för det internationella försvarsunderrättelse- och säkerhetssamarbetet eller det annars är nödvändigt för verksamheten.

2 kap. Försvarsmaktens databaser

Inledande bestämmelse

1 § I försvarsunderrättelseverksamheten och den militära säkerhetstjänsten skall det finnas ett antal skilda samlingar uppgifter, som med hjälp av automatiserad behandling används gemensamt

i verksamheten för de i 1 kap. 5–7 §§ angivna ändamålen (databaser).

Informationsdatabasen

2 § Uppgifter som samlats in från öppna källor skall behandlas i en informationsdatabas för att göra insamlad information tillgänglig i verksamheten.

Uppgifter i databasen får utöver vad som framgår av första stycket behandlas endast genom att föras över till en underrättelse- och säkerhetsdatabas.

Underrättelse- och säkerhetsdatabasen

3 § Uppgifter som samlats in på annat sätt än från öppna källor skall lagras i en underrättelse- och säkerhetsdatabas.

I databasen får även lagras uppgifter som överförts från informationsdatabasen.

4 § Uppgifter får behandlas i databasen för analys och bearbetning av inhämtat underrättelsematerial samt för lagring och delgivning av underrättelserapporter.

Uppgifter som får behandlas

5 § Regeringen, eller den myndighet regeringen bestämmer, meddelar närmare föreskrifter eller beslut om vilka uppgifter som får behandlas i databaserna.

I 1 kap. 7 § finns vissa bestämmelser om innehåll som gäller för uppgifter som behandlas i den militära säkerhetstjänsten.

Sökbegrepp

6 § Vid sökning efter uppgifter i informationsdatabasen eller underrättelse- och säkerhetsdatabasen får uppgifter om ras eller etniskt ursprung, politisk åsikt, religiös eller filosofisk övertygelse, medlemskap i fackförening, hälsa eller sexualliv användas som sökbegrepp endast om det är nödvändigt för syftet med behandlingen.

Direktåtkomst

7 § Vilka som får ha direktåtkomst till Försvarmaktens informationsdatabas eller underrättelse- och säkerhetsdatabas bestäms av regeringen i förordning eller beslut.

Regeringen, eller den myndighet regeringen bestämmer, meddelar närmare föreskrifter eller beslut om omfattningen av direktåtkomsten.

3 kap. Enskildas rättigheter

Information till den registrerade

1 § Vid tillämpningen av denna lag gäller bestämmelserna om information till den registrerade i 23 och 25–27 §§ personuppgiftslagen (1998:204).

Rättelse och skadestånd

2 § Bestämmelserna i personuppgiftslagen (1998:204) om rättelse och skadestånd gäller vid behandling av personuppgifter enligt denna lag eller anslutande författningar.

Överklagande

3 § Försvarsmaktens beslut om rättelse och om information som skall lämnas enligt 26 § personuppgiftslagen (1998:204) får överklagas hos allmän förvaltningsdomstol. Andra beslut enligt denna lag får inte överklagas.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Särskild granskning till skydd för den personliga integriteten

4 § Den myndighet som regeringen bestämmer skall ha till särskild uppgift att granska att Försvarsmaktens behandling av personuppgifter i försvarsunderrättelseverksamheten och den militära säkerhetstjänsten sker i enlighet med bestämmelserna i denna lag.

1. Denna lag träder i kraft den 1 juli 2004.

2. Bestämmelser i lagen om grundläggande krav på behandling av personuppgifter samt behandling av känsliga personuppgifter skall inte börja tillämpas förrän den 1 oktober 2007 i fråga om sådan manuell behandling av personuppgifter som påbörjats före den 24 oktober 1998 eller manuell behandling som utförs för ett visst bestämt ändamål om manuell behandling för ändamålet påbörjats före den 24 oktober 1998.

2 Förslag till lag om behandling av uppgifter i Försvarets radioanstalts underrättelseverksamhet

Härigenom föreskrivs följande.

1 kap. Allmänna bestämmelser

Lagens tillämpningsområde m.m.

1 § Denna lag tillämpas vid behandling av personuppgifter i Försvarets radioanstalts underrättelseverksamhet, om behandlingen är helt eller delvis automatiserad eller om uppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

Bestämmelserna i 4–5 §§ samt 2 kap. gäller även vid behandling av uppgifter om juridiska personer.

I 2 kap. finns bestämmelser om behandling av personuppgifter i Försvarets radioanstalts databaser.

Förhållandet till personuppgiftslagen

2 § Om inte annat anges i 3 § eller i 3 kap. gäller denna lag i stället för personuppgiftslagen (1998:204).

3 § När personuppgifter behandlas enligt denna lag eller enligt andra föreskrifter i det ämne som regleras i lagen gäller personuppgiftslagens (1998:204) bestämmelser om

1. definitioner i 3 §,
2. förhållandet till offentlighetsprincipen m.m. i 8 §,
3. grundläggande krav på behandling i 9 §,
4. säkerheten vid behandling i 30 och 31 §§,

5. personuppgiftsombud m.m. i 36 § andra stycket och 38–40 §§,
6. tillsynsmyndighetens befogenheter i 43 och 47 §§, och
7. straff i 49 §.

Personuppgiftsansvar

4 § Försvarets radioanstalt är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför eller som det åligger myndigheten att utföra. Motsvarande ansvar gäller för behandling av uppgifter om juridiska personer.

Ändamål

5 § Uppgifter får behandlas i underrättelseverksamheten dels för att kartlägga yttre militära hot mot landet dels till stöd för svensk utrikes-, försvars- och säkerhetspolitik, om det behövs för

1. säkerhetspolitiska och militärstrategiska bedömningar,
2. analyser av pågående och bedömda framtida konflikter, eller
3. biografisk försvarsunderrättelseverksamhet.

Uppgifter får också behandlas om det behövs för myndighetens verksamhet med att

1. bedriva signalspaning enligt den inriktning som regeringen, Försvarsmakten och övriga uppdragsgivare anger,
2. följa förändringen av signalmiljön i omvärlden, den tekniska utvecklingen och signalskyddet,
3. fortlöpande utveckla den teknik och metodik som behövs för att bedriva verksamheten,
4. utföra matematiska bedömningar av kryptosystem för totalförsvaret, samt
5. biträda andra myndigheter vid värdering, utveckling, anskaffning och drift av signalspaningssystem.

Behandling av känsliga personuppgifter

6 § Uppgifter om en person får inte behandlas enbart på grund av vad som är känt om personens ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexualliv.

Om uppgifter om en person behandlas på annan grund får de kompletteras med sådana uppgifter som avses i första stycket om det är nödvändigt för syftet med behandlingen.

Överföring av personuppgifter till tredje land

7 § Personuppgifter som behandlas med stöd av denna lag får lämnas ut till andra länder om sekretess inte hindrar det och det behövs för att Försvarets radioanstalt skall kunna fullgöra sina uppgifter inom ramen för det internationella försvarsunder rättelse- och säkerhetssamarbetet eller det annars är nödvändigt för verksamheten.

2 kap. Försvarets radioanstalts databaser

Inledande bestämmelse

1 § I underrättelseverksamheten skall det finnas ett antal skilda samlingar uppgifter, som med hjälp av automatiserad behandling används gemensamt i verksamheten för de i 1 kap. 5 § angivna ändamålen (databaser).

Urvalsdatabasen

2 § Uppgifter som används för att bestämma planering och inriktning av inhämtning av information, genom signalspaning eller på annat sätt, skall behandlas i en urvalsdatasas.

Uppgifter i databasen får endast behandlas för tillhandahållande av nödvändig urvalsinformation.

Källdatabasen

3 § Uppgifter som har inhämtats genom signalspaning skall behandlas i en källdatabas för att göra inhämtad information tillgänglig i verksamheten.

Uppgifter i databasen får utöver vad som anges i första stycket behandlas endast genom att med hjälp av urvalskriterier föras över till analysdatabasen.

Databasen för öppna källor

4 § Uppgifter som har inhämtats på annat sätt än genom signalspaning skall behandlas i en databas för öppna källor för att göra inhämtad information tillgänglig i verksamheten.

Uppgifter i databasen får utöver vad som anges i första stycket behandlas endast genom att med hjälp av urvalskriterier föras över till analysdatabasen.

Analysdatabasen

5 § Uppgifter som lagras i källdatabasen och databasen för öppna källor får tillsammans med andra nödvändiga uppgifter behandlas i en analysdatabas för analys och annan bearbetning, såsom dekryptering och översättning.

Uppgifter i databasen får utöver vad som framgår av första stycket behandlas endast för utarbetande av underrättelserapporter och lagring av arbetsmaterial för sådana rapporter.

Rapportdatabasen

6 § Uppgifter i färdiga underrättelserapporter som har utarbetats i analysdatabasen skall behandlas i en rapportdatabas för att göra informationen i rapporterna tillgänglig i verksamheten.

Uppgifter som får behandlas

7 § Regeringen, eller den myndighet regeringen bestämmer, meddelar närmare föreskrifter eller beslut om vilka uppgifter som får behandlas i databaserna.

Sökbegrepp

8 § Vid sökning efter uppgifter i en databas får uppgifter om ras eller etniskt ursprung, politisk åsikt, religiös eller filosofisk övertygelse, medlemskap i fackförening, hälsa eller sexualliv användas som sökbegrepp endast om det är nödvändigt för syftet med behandlingen.

Direktåtkomst

9 § Direktåtkomst får förekomma endast till rapportdatabasen. Regeringen meddelar närmare föreskrifter eller beslut om vilka som får ha direktåtkomst till rapportdatabasen.

Regeringen, eller den myndighet regeringen bestämmer, meddelar närmare föreskrifter eller beslut om omfattningen av direktåtkomsten.

3 kap. Enskildas rättigheter m.m.

Information till den registrerade

1 § Vid tillämpningen av denna lag gäller bestämmelserna om information till den registrerade i 23 och 25–27 §§ personuppgiftslagen (1998:204).

Rättelse och skadestånd

2 § Bestämmelserna i personuppgiftslagen (1998:204) om rättelse och skadestånd gäller vid behandling av personuppgifter enligt denna lag eller anslutande författningar.

Överklagande

3 § Försvarets radioanstalts beslut om rättelse och om information som skall lämnas enligt 26 § personuppgiftslagen (1998:204) får överklagas hos allmän förvaltningsdomstol. Andra beslut enligt denna lag får inte överklagas.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Särskild granskning till skydd för den personliga integriteten

4 § Den myndighet som regeringen bestämmer skall ha till särskild uppgift att granska att Försvarets radioanstalts behandling av personuppgifter i underrättelseverksamheten sker i enlighet med bestämmelserna i denna lag.

1. Denna lag träder i kraft den 1 juli 2004.

2. Bestämmelser i lagen om grundläggande krav på behandling av personuppgifter samt behandling av känsliga personuppgifter skall inte börja tillämpas förrän den 1 oktober 2007 i fråga om sådan manuell behandling av personuppgifter som påbörjats före den 24 oktober 1998 eller manuell behandling som utförs för ett visst bestämt ändamål om manuell behandling för ändamålet påbörjats före den 24 oktober 1998.

3 Förslag till lag om ändring i sekretesslagen (1980:100)

Härigenom föreskrivs att det i sekretesslagen (1980:100) skall införas en ny paragraf, 9 kap. 27 §, av följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

9 kap.

27 §

Sekretess gäller hos Försvarsmakten i den militära under rättelse- och säkerhetstjänsten för uppgift om enskilds personliga eller ekonomiska förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon honom närstående lider skada eller men.

I fråga om uppgift i allmän handling gäller sekretessen i högst sjuttio år.

Denna lag träder i kraft den 1 juli 2004.

Bilaga 3

Förteckning över remissinstanser som har yttrat sig över Underrättelsedatautredningens betänkande (SOU 2003:34)

Riksdagens ombudsmän, Justitiekanslern, Hovrätten för Övre Norrland, Kammarrätten i Stockholm, Länsrätten i Uppsala län, Rikspolisstyrelsen, Säkerhetspolisen, Registernämnden, Datainspektionen, Försvarmakten, Försvarets radioanstalt, Försvarets materielverk, Försvarets underrättelsenämnd, Totalförsvarets forskningsinstitut, Krisberedskapsmyndigheten, Kustbevakningen, Statens räddningsverk, Tullverket, Riksarkivet, Uppsala universitet och Göteborgs universitet.