Behandlingen av personuppgifter vid Försvarsmakten och Försvarets radioanstalt

Betänkande av Utredningen om behandlingen av personuppgifter vid Försvarsmakten och Försvarets radioanstalt

Stockholm 2018

STATENS OFFENTLIGA UTREDNINGAR

SOU 2018:63

SOU och Ds kan köpas från Norstedts Juridiks kundservice.
Beställningsadress: Norstedts Juridik, Kundservice, 106 47 Stockholm
Ordertelefon: 08-598 191 90
E-post: kundservice@nj.se
Webbadress: www.nj.se/offentligapublikationer

För remissutsändningar av SOU och Ds svarar Norstedts Juridik AB
på uppdrag av Regeringskanslients förvaltningsavdelning.
Svara på remiss – hur och varför
Statsrådsberedningen, SB PM 2003:2 (reviderad 2009-05-02).
En kort handledning för dem som ska svara på remiss.
Häftet är gratis och kan laddas ner som pdf från eller beställas på regeringen.se/remisser

Layout: Kommittéservice, Regeringskansliet
Omslag: Elanders Sverige AB
Tryck: Elanders Sverige AB, Stockholm 2018

ISBN 978-91-24849-2
ISSN 0375-250X

Till statsrådet och chefen för Försvarsdepartementet

Regeringen beslutade den 27 april 2017 att tillkalla en särskild utredare med uppdrag att göra en översyn av den lagstiftning som gäller för personuppgiftsbehandling inom Försvarsmakten och Försvarets radioanstalt. Syftet med uppdraget är att säkerställa att lagstiftningen är anpassad till den tekniska och legala utvecklingen.

Som särskild utredare förordnades samma dag f.d. generaldirektören och chefen för Försvarets radioanstalt Ingvar Åkesson.

Som sakkunniga i utredningen förordnades samma dag ämnesrådet och biträdande enhetschefen Mikael Andersson, Försvarsdepartementet och kanslirådet Eva Larsson Behrmann, Försvarsdepartementet.

Som experter att biträda utredningen förordnades den 2 juni 2017 chefsjuristen Michaela Dràb, Försvarets radioanstalt, avdelningschefen Stefan Vestergren, Försvarsmakten, sektionschefen Annika Grahn Sulusi, Försvarsmakten och avdelningsdirektören Christer Hellsten, Försvarets radioanstalt.

Som sekreterare anställdes den 29 maj 2017 hovrättsassessorn Alexander Lundén.

Utredningen har antagit namnet Utredningen om behandlingen av personuppgifter vid Försvarsmakten och Försvarets radioanstalt.

Härmed överlämnas betänkandet *Behandlingen av personuppgifter vid Försvarsmakten och Försvarets radioanstalt* (SOU 2018:63). Uppdraget är härmed slutfört.

Stockholm i juli 2018

Ingvar Åkesson

/Alexander Lundén

Innehåll

Bilagor

Sammanfattning

Uppdraget

Sedan nuvarande särskilda regler för personuppgiftsbehandling i Försvarsmaktens och Försvarets radioanstalts verksamheter trädde i kraft år 2007 har det skett en omfattande utveckling och ett reformarbete på personuppgiftsområdet. Bl.a. har Europeiska unionen (EU) enats om en genomgripande dataskyddsreform som genomfördes under våren 2018. Reformen omfattade dels en allmän dataskyddsförordning, dels ett dataskyddsdirektiv som behandlar dataskyddet vid bl.a. brottsbekämpning, lagföring och straffverkställighet. En konsekvens av EU:s reform är att den svenska personuppgiftslagen har upphävts och att all personuppgiftslagstiftning som anknyter till denna lag därför behöver ses över och anpassas.

Verksamheter inom försvar och nationell säkerhet är uttryckligen undantagna från EU:s lagstiftningskompetens. Viss verksamhet vid Försvarsmakten och Försvarets radioanstalt regleras emellertid för närvarande av personuppgiftslagen, varför denna utredning fick i uppdrag bl.a. att göra en översyn av de författningar som reglerar personuppgiftsbehandling inom Försvarsmakten och Försvarets radioanstalt. Utredningen fick även i uppdrag att analysera huruvida rådande lagstiftning är ändamålsenlig för Försvarsmaktens och Försvarets radioanstalts verksamheter och om den är tillräcklig i fråga om skyddet för enskildas personliga integritet.

Anpassningar och andra ändringar genom två nya lagar

Tillämpningsområdet

Utredningen föreslår att viss, särskilt angiven verksamhet hos Försvarsmakten och Försvarets radioanstalt även fortsättningsvis ska särregleras i två nya heltäckande och självständiga lagar. Utredningen föreslår samtidigt ett antal ändringar i förhållande till nuvarande regler för personuppgiftsbehandling hos de båda myndigheterna. Bl.a. vidgas tillämpningsområdet för vilka verksamheter hos de båda myndigheterna som omfattas av den särskilda lagregleringen.

Tillåtna rättsliga grunder och behandling för nya ändamål

Som anförts ovan föreslår utredningen vidgade tillämpningsområden för de båda nya lagarna jämfört med nuvarande lagstiftning. De nya lagarna innehåller emellertid också tydliga och uttömmande rättsliga grunder som anger vilka personuppgiftsbehandlingar som omfattas av de båda nya lagarna. För Försvarets radioanstalt införs dessutom bestämmelser om s.k. preciserad finalitet, vilket innebär förbättrad förutsägbarhet om i vilka syften Försvarets radioanstalt får vidarebehandla inhämtade uppgifter.

Rättslig grund för Försvarsmakten – Sveriges försvar och säkerhet

Personuppgiftsbehandling inom Försvarsmaktens huvuduppgifter bör omfattas av en svensk nationell reglering. Försvarsmakten föreslås därför få behandla personuppgifter om det är nödvändig för att planera, förbereda och genomföra verksamhet som rör Sveriges försvar och säkerhet eller internationellt försvars- och säkerhetssamarbete. Uppgiften att bedriva sådan verksamhet ska följa av lag, förordning eller ett särskilt beslut i vilket regeringen har uppdragit åt myndigheten att utföra uppgiften.

Försvarsmakten har bl.a. i uppdrag att upprätthålla och utveckla ett militärt försvar som ytterst kan möta ett väpnat angrepp samt att försvara Sverige och främja svensk säkerhet. Vid höjd beredskap ska Försvarsmakten kunna krigsorganisera, mobilisera och använda alla krigsförband för att möta ett militärt hot mot Sverige och svenska intressen. Krigsorganisationen och planeringen av denna innefattar

personuppgiftsbehandling av anställda i Försvarsmakten och andra som på annat sätt är knutna till myndigheten. När Försvarsmakten planerar, förbereder och genomför militära operationer och övningar behandlar myndigheten också uppgifter om de som deltar i operationerna och övningarna. Personuppgiftsbehandling inom underrättelseverksamhet för att lösa Försvarsmaktens militära uppgifter, som inte utgör försvarsunderrättelseverksamhet eller militär säkerhetstjänst, omfattas av bestämmelsen om den rättsliga grunden, liksom att pröva och anpassa teknisk utrustning och tekniska system. Den rättliga grunden ger Försvarsmakten det stöd för personuppgiftsbehandling enligt den föreslagna lagen som krävs inom bl.a. dessa verksamheter.

Rättsliga grunder för Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst

Med vissa ändringar innehåller den föreslagna lagen om behandling av personuppgifter vid Försvarsmakten i huvudsak samma rättsliga grunder för myndighetens försvarsunderrättelseverksamhet och militära säkerhetstjänst som i nuvarande lagstiftning. Kravet att uppgifter om en person får behandlas i försvarsunderrättelseverksamheten endast om personen har anknytning till en preciserad inriktning för försvarsunderrättelseverksamheten tas dock bort.

Rättsliga grunder för Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet

Också för denna verksamhet innehåller den föreslagna lagen om behandling av personuppgifter vid Försvarets radioanstalt samma rättsliga grunder som i nuvarande lagstiftning. Kravet att uppgifter om en person får behandlas i försvarsunderrättelseverksamheten endast om personen har anknytning till en preciserad inriktning för försvarsunderrättelseverksamheten tas dock bort.

Rättslig grund för Försvarets radioanstalts informationssäkerhetsverksamhet

Av Försvarets radioanstalts instruktion framgår att Försvarets radioanstalt har i uppdrag att vara statens resurs för teknisk informationssäkerhet och ska ha hög kompetens inom informationssäkerhetsområdet. Förslaget till lag om behandling av personuppgifter vid Försvarets radioanstalt innehåller en rättslig grund som innebär att personuppgifter får behandlas i Försvarets radioanstalts informationssäkerhetsverksamhet om det är nödvändigt för att kunna skydda den egna myndigheten eller för att kunna stödja andra verksamheter som är av betydelse för Sveriges säkerhet. Uppgiften att lämna stöd till andra verksamheter ska följa av lag eller förordning eller regeringsbeslut i ett enskilt fall.

Det finns även ett antal tillkommande ändamål för vilka personuppgifter som behandlas i informationssäkerhetsverksamheten bör få behandlas. Personuppgiftsbehandling föreslås få ske om det är nödvändigt för att tillhandahålla information som behövs hos den som tar emot uppgifter om informationssäkerhet samt om det är nödvändigt för att tillhandahålla information som behövs med anledning av samverkan med andra som verkar på informationssäkerhetsområdet såväl inom som utom landet. Detta bör dock bara få ske i den utsträckning det följer av lag eller förordning eller om regeringen i ett enskilt fall beslutar om det.

En nära samverkan mellan försvarsunderrättelseverksamheten och informationssäkerhetsverksamheten är enligt utredningen av stor betydelse. För underrättelseverksamheten är det angeläget att kunna ta del av uppgifter från informationssäkerhetsverksamheten när det gäller att kartlägga allvarliga yttre hot mot samhällets infrastruktur och främmande underrättelseverksamhet. Personuppgifter förslås därför även få behandlas om det är nödvändigt för att tillhandahålla information av detta slag.

Informationssäkerhetsverksamheten är även av betydelse för utvecklingsverksamheten. Personuppgifter som får behandlas i informationssäkerhetsverksamheten förslås därför även få behandlas om det är nödvändigt för att tillhandahålla information som behövs i utvecklingsverksamheten.

Behandling av personuppgifter i allmänt tillgänglig information

För att kunna bedriva en effektiv försvarsunderrättelseverksamhet utöver den information som inhämtas genom hemliga metoder behöver både Försvarsmakten och Försvarets radioanstalt också tillgång till allmänt tillgänglig information. Allmänt tillgänglig information kan vara personuppgifter som kan påträffas vid sökning på internet eller vid sökningar i öppna databaser. Uppgifterna kan vara gratis eller tillgängliga på kommersiell grund. Det kan också röra sig om uppgifter som t.ex. en abonnent på ett eller annat sätt har samtyckt att uppgifterna finns med i elektroniska telefonkataloger eller förteckningar över ip-adresser i olika länder

Personuppgifter som utgör allmänt tillgänglig information föreslås därför få behandlas av Försvarsmakten om det är nödvändigt för planering, förberedelse och genomförande av verksamhet som rör Sveriges försvar och säkerhet eller internationellt försvars- och säkerhetssamarbete, försvarsunderrättelseverksamheten, eller den militära säkerhetstjänsten. Motsvarande föreslås för Försvarets radioanstalt om det är nödvändigt för de ändamål som anges för försvarsunderrättelse- och utvecklingsverksamheten och informationssäkerhetsverksamheten.

Behandling av känsliga personuppgifter

De föreslagna lagarna, liksom de nuvarande, förbjuder behandling av personuppgifter som grundar sig enbart på känsliga personuppgifter. Författningarna innehåller undantag från förbudet genom att andra uppgifter får kompletteras med känsliga uppgifter och att känsliga personuppgifter får användas som sökbegrepp om det är absolut nödvändigt. Känsliga personuppgifter i form av biometriska uppgifter får emellertid behandlas självständigt, medan behandling av genetiska uppgifter föreslås vara helt förbjudet för båda myndigheterna.

Känsliga personuppgifter föreslås emellertid få behandlas utan hinder av dessa regler om den som personuppgifterna rör har lämnat sitt uttryckliga samtycke eller på ett tydligt sätt har offentliggjort uppgifterna. Detta ska dock inte gälla genetiska uppgifter.

Längsta tid för behandling

De föreslagna lagarna reglerar längsta tid för behandling, men innehåller inte – som de nuvarande – regler om bevarande och gallring. Lagarna syftar nämligen till att skydda den personliga integriteten och reglerar inte bevarande och gallring i arkivlagens mening. Jämfört med nuvarande bestämmelser har de därför formuleras om så att det framgår att det är fråga om dataskyddsbestämmelser. Regleringen ska utgå från hur länge personuppgifter får behandlas.

Utökade möjligheter till elektroniskt utlämnande

Regleringen av i vilken utsträckning personuppgifter får lämnas ut på medium för automatiserad behandling moderniseras för att möta de ökade behoven av att kunna kommunicera elektroniskt. För Försvarsmakten blir det tillåtet att lämna ut personuppgifter elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt, medan utlämnande från Försvarets radioanstalt är fortsatt mer restriktivt.

Försvarsmakten och Försvarets radioanstalt ska få medge varandra och Säkerhetspolisen direktåtkomst till personuppgifter som har gjorts gemensamt tillgängliga och som behandlas för vissa syften. Även utländska underrättelse- och säkerhetstjänster kan få medges direktåtkomst till uppgifter som Försvarsmakten behandlar för vissa syften, om det t.ex. behövs för samarbetet mot terrorism. Sådan direktåtkomst ska dock endast få medges till personuppgifter i en avskild uppgiftssamling och endast om svenska intressen kan motivera det.

Tillsyn över myndigheternas personuppgiftsbehandling

Både Datainspektionen och Statens inspektion för försvarsunderrättelseverksamheten ska på samma sätt som i dag utöva tillsyn och kontroll över Försvarsmaktens och Försvarets radioanstalts personuppgiftsbehandling.

Konsekvenser för den personliga integriteten

Sammantaget innebär förslagen att skyddet för den personliga integriteten kommer att vara på samma nivå som för närvarande. I viss mån kan intrånget i personlig integritet öka genom de ökade möjligheterna till direktåtkomst som motiveras av starka försvars- och säkerhetsintressen.

Ikraftträdande och övergångsbestämmelser

De nya författningarna och ändringarna i de befintliga författningarna föreslås träda i kraft den 1 oktober 2019. Det krävs särskilda övergångsbestämmelser för bestämmelserna om loggning i uppgiftssamlingar. Till de nya lagarna krävs det också övergångsbestämmelser för ärenden om tillsyn eller granskning som rör behandlingen av personuppgifter som har påbörjats före ikraftträdandet men inte hunnit slutföras.

Förkortningar m.m.

2016 års dataskydds-direktiv	Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF
brottsdatalagen	Brottsdatalagen (2018:1177)
dataskyddsdirektivet	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
dataskydds-förordningen	Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)
dataskydds-konventionen	Europarådets konvention av den 28 januari 1981 om skydd för enskilda vid automatisk databehandling av personuppgifter

dataskyddslagen	Lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning
dataskyddsrambeslutet	Rådets rambeslut 2008/977/RIF av den 27 november 2008 om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete
DI	Datainspektionen
dir.	direktiv
dnr	diarienummer
EU	Europeiska unionen
Europadomstolen	Europeiska domstolen för de mänskliga rättigheterna
Europakonventionen	Europeiska konventionen den 4 november 1950 angående skydd för de mänskliga rättigheterna och de grundläggande friheterna
EU-stadgan	Europeiska unionens stadga om de grundläggande rättigheterna
f./ff.	följande sida/sidor
FM	Försvarsmakten
FM-PuF	förordningen (2007:260) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst

FM-PuL	Lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst
FN	Förenta nationerna
FRA	Försvarets radioanstalt
FRA-PuF	förordningen (2007:261) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet
FRA-PuL	lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet
FUL	lagen (2000:130) om försvarsunderrättelseverksamhet
Fö	Försvarsdepartementet
IKFN	förordningen (1982:765) om Försvarsmaktens ingripanden vid kränkningar av Sveriges territorium under fred och neutralitet m.m.
JO	Riksdagens ombudsmän
JK	Justitiekanslern
KU	Konstitutionsutskottet
MSB	Myndigheten för samhällsskydd och beredskap

NCT	Nationellt centrum för terrorhotbedömning
OSL	offentlighets- och sekretesslagen (2009:400)
prop.	regeringens proposition
PUL	personuppgiftslagen (1998:204)
RA-FS	Riksarkivets författningssamling
RA-MS	Riksarkivets myndighetsspecifika föreskrifter
rskr.	Riksdagsskrivelse
Signalspaningslagen	lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet
Siun	Statens inspektion för försvarsunderrättelseverksamheten
SOU	Statens offentliga utredningar
TDV	Tekniskt detekterings- och varningssystem
TF	Tryckfrihetsförordningen (1949:105)

1 Författningsförslag

1.1 Förslag till lag (2019:000) om behandling av personuppgifter vid Försvarsmakten

Härigenom föreskrivs följande.

1 kap. Allmänna bestämmelser

Syftet med lagen

1 § Syftet med denna lag är att säkerställa att Försvarsmakten kan behandla personuppgifter på ett ändamålsenligt sätt och att skydda fysiska personers grundläggande fri- och rättigheter i samband med sådan behandling.

Lagens tillämpningsområde

2 § Denna lag gäller vid Försvarsmaktens behandling av personuppgifter som rör Sveriges försvar och säkerhet.

3 § Lagen gäller vid sådan behandling av personuppgifter som 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.

4 § Vid behandling av personuppgifter enligt denna lag gäller inte lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

Förhållandet till annan reglering

5 § Bestämmelserna i denna lag ska inte tillämpas i den utsträckning det skulle inskränka skyldigheten enligt 2 kap. tryckfrihetsförordningen att lämna ut personuppgifter.

Personuppgiftsansvar

6 § Försvarsmakten är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför.

Personuppgiftsansvaret omfattar all behandling av personuppgifter som utförs under myndighetens ledning eller på dess vägnar.

7 § Försvarsmakten får vara gemensamt personuppgiftsansvarig med annan endast i den utsträckning det följer av lag eller förordning eller om regeringen i ett enskilt fall beslutar om det.

Definitioner

8 § I denna lag används följande uttryck med nedan angiven betydelse.

Uttryck	*Betydelse*
Behandling av personuppgifter	En åtgärd eller kombination av åtgärder som vidtas i fråga om personuppgifter eller uppsättningar av personuppgifter, oavsett om det görs automatiserat eller inte, t.ex. insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämnande, spridning eller tillhandahållande på annat sätt, justering, sammanföring, begränsning, radering eller förstöring.

Biometriska uppgifter	Personuppgifter som rör en persons fysiska, fysiologiska eller beteendemässiga kännetecken, som tagits fram genom särskild teknisk behandling och som möjliggör eller bekräftar unik identifiering av personen i fråga.
Dataskyddsombud	En fysisk person som utses av den personuppgiftsansvarige för att självständigt se till att personuppgifter behandlas författningsenligt och på ett korrekt sätt.
Genetiska uppgifter	Personuppgifter som rör en persons nedärvda eller förvärvade genetiska kännetecken och som härrör från analys av ett spår av eller ett prov från personen i fråga.
Logg	Behandlingshistorik som sparas viss tid.
Mottagare	Den till vilken personuppgifter lämnas ut, med undantag av en myndighet som med stöd av författning utövar tillsyn, kontroll eller revision.
Personuppgift	Varje upplysning om en identifierad eller identifierbar fysisk person som är i livet.
Personuppgiftsansvarig	Den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter.

Personuppgiftsbiträde	Den som, med stöd av ett skriftligt avtal eller annan skriftlig överenskommelse, behandlar personuppgifter för den personuppgiftsansvariges räkning.
Tredje part	Någon annan än den som personuppgiften rör, personuppgiftsansvarige, dataskyddsombudet, personuppgiftsbiträdet och sådana personer som under den personuppgiftsansvariges eller personuppgiftsbiträdets direkta ansvar har rätt att behandla personuppgifter.
Uppgiftssamling	En samling med uppgifter som med hjälp av automatiserad behandling är gemensamt tillgängliga.

2 kap. Behandling av personuppgifter

Rättsliga grunder

Försvar och säkerhet

1 § Försvarsmakten får behandla personuppgifter om det är nödvändigt för att planera, förbereda och genomföra verksamhet som rör

1. Sveriges försvar och säkerhet, eller
2. internationellt försvars- och säkerhetssamarbete.

Försvarsmaktens uppgift att bedriva sådan verksamhet som anges i första stycket ska följa av lag, förordning eller ett särskilt beslut i vilket regeringen uppdragit åt myndigheten att utföra uppgiften.

Särskilt om försvarsunderrättelseverksamhet

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

3 § De personuppgifter som Försvarsmakten har fått tillgång till i myndighetens försvarsunderrättelseverksamhet får fortsatt behandlas i den verksamheten, om det behövs för att fullgöra den.

Vad som sägs i första stycket gäller endast om inget annat följer av denna lag eller förordning som regeringen har meddelat i anslutning till lagen.

Särskilt om militär säkerhetstjänst

4 § Personuppgifter får behandlas i Försvarsmaktens militära säkerhetstjänst för att upptäcka, förebygga och avvärja säkerhetshotande verksamhet som riktas mot Försvarsmakten och dess säkerhetsintressen, om det är nödvändigt för att

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

5 § Uppgifter om en person får behandlas för de ändamål som anges i 4 § endast om

1. uppgifterna är nödvändiga för att kartlägga verksamhet som innefattar brott som kan hota Sveriges säkerhet eller terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott eller motsvarande brottslighet enligt tidigare lagstiftning,
2. uppgifterna är nödvändiga för att kartlägga underrättelseverksamhet riktad mot Försvarsmakten och dess säkerhetsintressen,
3. uppgifterna är nödvändiga för att kartlägga annan säkerhetshotande verksamhet än som avses i 1 och som innefattar brott eller åsidosättande av åligganden i anställning hos Försvarsmakten, och det finns särskilda skäl till att uppgiften ska 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 säkerhetsprövning enligt säkerhetsskyddslagen (1996:627) eller i annat fall är nödvändiga för att utföra en uppgift som rör säkerhetsskydd.

6 § Personuppgifter som behandlas enligt 5 § ska förses med upplysning om på vilken av de angivna grunderna uppgiften behandlas. Om behandlingen av en personuppgift föranleds av något annat än antagande om att personen har utövat eller kommer att utöva brottslig verksamhet ska 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 ska förses med en särskild upplysning om detta, om det inte på annat sätt klart framgår att sådant antagande inte finns.

Personuppgifter som behandlas enligt 5 § första stycket 1–3 ska i förekommande fall förses med en upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak.

7 § Trots vad som sägs i 5 och 6 §§ får personuppgifter som ingår i eller har uppkommit i samband med användning av totalförsvarets telekommunikations- och informationssystem behandlas för att förhindra obehörig insyn i och påverkan av dessa system. Det gäller även sådana uppgifter som avses i 15, 16, 18 och 19 §§. Behandling som särskilt syftar till att identifiera en person får dock endast utföras om bestämmelserna i 5 § 1, 2 eller 3 tillämpas.

Övriga rättsliga grunder

8 § Personuppgifter som utgör allmänt tillgänglig information får behandlas av Försvarsmakten om det är nödvändigt för de ändamål som anges i 1, 2 och 4 §§.

9 § Personuppgifter får behandlas av Försvarsmakten om det är nödvändigt för diarieföring, arkivering, handläggning av ett ärende eller för att utföra annan liknande uppgift som åligger myndigheten.

10 § Försvarsmakten får behandla personuppgifter för vetenskapliga, statistiska eller historiska ändamål inom denna lags tillämpningsområde.

11 § Försvarsmakten får behandla personuppgifter för att kunna tillgodose enskildas behov av information enligt 5 kap. och kunna lämna information vid tillsyn eller kontroll.

Grundläggande krav

Ändamål

12 § Personuppgifter får bara behandlas för särskilda, uttryckligt angivna och berättigade ändamål.

Personuppgifter får inte behandlas för något ändamål som är oförenligt med det ändamål för vilket personuppgifterna ursprungligen behandlades.

Författningsenlig och korrekt behandling

13 § Personuppgifter ska behandlas författningsenligt och på ett korrekt sätt.

Personuppgifternas kvalitet

14 § Personuppgifter som behandlas ska vara adekvata och relevanta i förhållande till ändamålen med behandlingen och, om det är nödvändigt, uppdaterade.

Uppgifter som beskriver en persons utseende ska utformas på ett objektivt sätt med respekt för människovärdet.

Fler personuppgifter får inte behandlas än vad som är nödvändigt med hänsyn till ändamålen med behandlingen.

Känsliga personuppgifter

15 § Personuppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening eller som rör hälsa, sexualliv eller sexuell läggning får inte behandlas.

När uppgifter om en person behandlas får de dock kompletteras med sådana uppgifter som avses i första stycket, om det är absolut nödvändigt för syftet med behandlingen.

16 § Biometriska uppgifter får behandlas endast om det är absolut nödvändigt för ändamålet för behandlingen. Genetiska uppgifter får inte behandlas.

17 § Vid sökning får personuppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening eller som rör hälsa, sexualliv eller sexuell läggning användas som sökbegrepp om det är absolut nödvändigt för syftet med behandlingen. Detsamma gäller biometriska uppgifter.

Personnummer

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

1. ändamålet med behandlingen,
2. vikten av en säker identifiering, eller
3. något annat beaktansvärt skäl.

Om den som uppgifterna rör har offentliggjort uppgifterna eller lämnat sitt samtycke

19 § Utan hinder av vad som föreskrivs i 15, 16 och 18 §§ får personuppgifter behandlas, om den som personuppgifterna rör har lämnat sitt uttryckliga samtycke eller på ett tydligt sätt har offentliggjort uppgifterna.

Första stycket gäller inte genetiska uppgifter.

Behandling av personuppgifter i vissa fall

20 § Hantering av information som innebär behandling av personuppgifter ska inte anses oförenlig med bestämmelserna i 1, 2, 4, 5, 7, 8 och 12–16 §§ i det skede av behandlingen då det inte har kunnat fastställas vilka personuppgifter som informationen innehåller.

Längsta tid som personuppgifter får behandlas

21 § Personuppgifter som behandlas automatiserat får inte behandlas under längre tid än vad som behövs för något eller några av de ändamål som anges i 1–11 §§.

Regeringen eller den myndighet regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter eller i ett enskilt fall besluta att personuppgifter får behandlas under endast viss tid eller bevaras för historiska, statistiska eller vetenskapliga ändamål.

Utlämnande av personuppgifter

22 § Personuppgifter som behandlas med stöd av denna lag får föras över till andra länder eller internationella organisationer endast om sekretess inte hindrar det och det är nödvändigt för att Försvarsmakten ska kunna fullgöra sina uppgifter inom ramen för internationellt försvars- och säkerhetssamarbete.

Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter eller i enskilt fall besluta att överföring får ske även i andra fall om det är nödvändigt för verksamheten vid Försvarsmakten.

23 § Personuppgifter får lämnas ut elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt.

Elektroniskt utlämnande genom direktåtkomst är tillåtet bara i den utsträckning som anges i 3 kap. 2–4 §§.

Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om begränsning av möjligheten att lämna ut personuppgifter elektroniskt enligt första stycket.

3 kap. Gemensamt tillgängliga uppgifter

Personuppgifter som får göras gemensamt tillgängliga

1 § Personuppgifter får göras gemensamt tillgängliga om det behövs för något av de ändamål som anges i 2 kap. Personuppgifter som endast ett fåtal personer har tillgång till anses inte som gemensamt tillgängliga.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter eller besluta i enskilda fall vilka uppgiftssamlingar som får finnas och vilka uppgifter som får behandlas i respektive uppgiftssamling.

Direktåtkomst

Försvarsunderrättelseverksamhet

2 § Trots sekretess enligt 38 kap. 4 § offentlighets- och sekretesslagen (2009:400) får Säkerhetspolisen och Försvarets radioanstalt medges direktåtkomst till personuppgifter som utgör bearbetningsunderlag och analysresultat inom försvarsunderrättelseverksamheten och som finns i uppgiftssamlingar.

3 § Om det behövs för samarbetet mot terrorism eller vid svenskt deltagande i annat internationellt underrättelse- och säkerhetssamarbete får, i den utsträckning det följer av lag eller förordning eller om regeringen i ett enskilt fall beslutat om det, en utländsk underrättelse- eller säkerhetstjänst medges direktåtkomst till personuppgifter som behandlas med stöd av 2 kap. 2 § och som finns i uppgiftssamlingar.

Direktåtkomst i andra fall

4 § Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter eller särskilt beslut om vilka som i andra fall än de som anges i 2 § och 3 § får ha direktåtkomst till gemensamt tillgängliga uppgifter.

Övriga bestämmelser

5 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela

1. ytterligare föreskrifter eller beslut i enskilda fall om omfattningen av direktåtkomsten, och
2. föreskrifter om behörighet och säkerhet vid sådan åtkomst.

4 kap. Skyldighet som personuppgiftsansvarig

Åtgärder för att säkerställa författningsenlig behandling

1 § Försvarsmakten ska, genom lämpliga tekniska och organisatoriska åtgärder, säkerställa att behandlingen av personuppgifter är författningsenlig och skydda rättigheterna för dem som uppgifterna rör.

2 § Försvarsmakten ska säkerställa att det förs loggar över personuppgiftsbehandling av gemensamt tillgängliga uppgifter. Regeringen eller den myndighet regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om loggar.

3 § Tillgången till personuppgifter ska alltid begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter.

Säkerheten för personuppgifter

4 § Försvarsmakten ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas, särskilt mot obehörig eller otillåten behandling eller förstöring och mot förlust eller annan oavsiktlig skada.

Dataskyddsombud

5 § Försvarsmakten ska inom myndigheten utse ett eller flera dataskyddsombud och anmäla till tillsynsmyndigheten när dataskyddsombud utses och entledigas.

6 § Dataskyddsombudet ska

1. självständigt kontrollera att Försvarsmakten behandlar personuppgifter författningsenligt och på ett korrekt sätt och i övrigt fullgör sina skyldigheter,
2. informera och ge råd till Försvarsmakten och till dem som behandlar personuppgifter under myndighetens ledning om deras skyldigheter vid behandling av personuppgifter,
3. samråda med tillsynsmyndigheten, och
4. föra en förteckning över de kategorier av behandlingar som Försvarsmakten ansvarar för och som är helt eller delvis automatiserade.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om vad en förteckning som avses i första stycket 4 ska innehålla.

Om Försvarsmakten bryter mot de bestämmelser som gäller för behandlingen av personuppgifter och rättelse inte vidtas, ska dataskyddsombudet anmäla det till tillsynsmyndigheten.

Personuppgiftsbiträden

7 § Försvarsmakten får, om det är lämpligt, anlita personuppgiftsbiträden för behandling av personuppgifter på Försvarsmaktens vägnar. Innan ett personuppgiftsbiträde anlitas, ska Försvarsmakten försäkra sig om att biträdet kommer att vidta de lämpliga tekniska och organisatoriska åtgärder som krävs för att behandlingen av personuppgifter ska vara författningsenlig och för att skydda rättigheterna för den som uppgifterna rör.

8 § Personuppgiftsbiträdets behandling av personuppgifter ska regleras i ett skriftligt avtal eller annan skriftlig överenskommelse.

9 § Ett personuppgiftsbiträde får inte anlita ett annat personuppgiftsbiträde utan skriftligt tillstånd av Försvarsmakten.

10 § Ett personuppgiftsbiträde eller den eller de personer som arbetar under biträdets eller Försvarsmaktens ledning ska behandla personuppgifter i enlighet med instruktioner från Försvarsmakten.

Om ett personuppgiftsbiträde, i strid med Försvarsmaktens instruktioner, bestämmer ändamålen med och medlen för behandlingen, ska biträdet anses vara personuppgiftsansvarig enligt denna lag för den behandlingen.

11 § Det som sägs om Försvarsmaktens skyldigheter i 2–4 §§ gäller även för personuppgiftsbiträden som Försvarsmakten anlitar.

5 kap. Enskildas rättigheter

Rätten till information

Allmän information

1 § Försvarsmakten ska göra följande allmänna information tillgänglig.

1. Myndighetens identitet och kontaktuppgifter.
2. Uppgifter om dataskyddsombudet.
3. Ändamålen med behandlingen.
4. Rätten enligt 3 § att begära att få information om behandling av personuppgifter och att få del av dem.
5. Rätten att begära rättelse, radering eller begränsning av behandlingen enligt 6 §.

Information som ska lämnas om uppgifterna samlas in från personen själv

2 § Om uppgifter om en person samlas in från personen själv, ska Försvarsmakten när personuppgifterna erhålls, självmant lämna följande information till den som uppgifterna rör:

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 som uppgifterna rör ska 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 som ska lämnas efter begäran

3 § Försvarsmakten är skyldig att en gång per kalenderår till den som begär det lämna skriftligt besked om personuppgifter som rör honom eller henne behandlas. Behandlas sådana uppgifter ska sökanden få del av dem och få följande skriftliga information.

1. Vilka personuppgifter om den sökande som behandlas.
2. Varifrån personuppgifterna kommer.
3. Den rättsliga grunden för behandlingen.
4. Ändamålen med behandlingen.
5. Mottagare eller kategorier av mottagare av personuppgifterna, även i annat land eller internationella organisationer.
6. Hur länge personuppgifterna får behandlas eller, om det inte är möjligt att ange, kriterierna för att fastställa det.
7. Rätten att begära rättelse, radering eller begränsning av behandlingen enligt 6 §.

Utlämnande enligt första stycket behöver inte omfatta personuppgifter som sökanden har tagit del av, om inte han eller hon begär det. Det ska dock framgå av informationen att personuppgifterna i fråga behandlas.

En ansökan enligt första stycket ska göras skriftligen hos Försvarsmakten och vara undertecknad av den sökande själv. Information enligt första stycket ska 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.

Begränsning av rätten till information

4 § Informationsskyldigheten i 2 och 3 §§ gäller inte i den utsträckning sekretess hindrar att uppgifterna lämnas ut.

Om förutsättningarna i första stycket är uppfyllda, är Försvarsmakten inte skyldig att lämna ut skälen för beslut enligt första stycket eller beslut i fråga om rättelse, radering eller begränsning av behandlingen enligt 6 §.

5 § Informationsskyldigheten i 2 och 3 §§ gäller inte personuppgifter i löpande text som inte fått sin slutliga utformning när begäran gjordes eller som utgör minnesanteckning eller liknande.

Informationsskyldigheten gäller dock om uppgifterna har lämnats ut till tredje part, behandlas enbart för vetenskapliga, statistiska eller historiska ändamål eller arkivändamål av allmänt intresse eller, när det gäller löpande text som inte fått sin slutliga utformning, om uppgifterna har behandlats längre än ett år.

Rätten till rättelse, radering och begränsning av behandlingen

6 § Försvarsmakten ska på begäran av den som personuppgiften rör snarast rätta, radera eller begränsa sådana personuppgifter som inte har behandlats i enlighet med denna lag eller föreskrifter som har meddelats med stöd av lagen.

Försvarsmakten ska också underrätta tredje part till vilken uppgifterna har lämnats ut om åtgärden, om den som personuppgiften rör begär det eller om en mera betydande skada eller olägenhet för denne skulle kunna undvikas genom en underrättelse.

Någon underrättelse behöver dock inte lämnas, om sekretess hindrar det eller detta är omöjligt eller skulle innebära en oproportionerligt stor arbetsinsats.

Avgiftsfri information

7 § Information enligt 1 och 2 §§ ska lämnas utan avgift.

Information och uppgifter enligt 3 § ska lämnas utan avgift en gång per kalenderår. Om någon begär information och uppgifter enligt 3 § oftare än en gång per kalenderår, får Försvarsmakten avslå begäran.

6 kap. Tillsyn

Tillsyn över personuppgiftsbehandlingen

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

Tillsynsmyndigheten ska ge råd och stöd till Försvarsmakten om myndighetens skyldigheter enligt lag eller annan författning eller när det i övrigt är påkallat.

Befogenheter

Utredningsbefogenheter

2 § Tillsynsmyndigheten har rätt att av Försvarsmakten eller ett personuppgiftsbiträde på begäran få

1. tillgång till personuppgifter som behandlas,
2. upplysningar om och dokumentation av behandlingen av personuppgifter och säkerhets- och skyddsåtgärder,
3. tillträde till sådana lokaler som har anknytning till behandling av personuppgifter och tillgång till utrustning och andra medel för behandling av personuppgifter, och
4. det biträde och annan information som behövs för tillsynen.

Förebyggande befogenheter

3 § Om tillsynsmyndigheten bedömer att det finns risk för att personuppgifter kan komma att behandlas i strid med lag eller annan författning, ska myndigheten genom råd, rekommendationer eller påpekanden försöka förmå Försvarsmakten eller personuppgiftsbiträdet att vidta åtgärder för att minska den risken.

Tillsynsmyndigheten får utfärda en skriftlig varning för att planerad behandling av personuppgifter riskerar att stå i strid med lag eller annan författning. Detsamma gäller om pågående behandling riskerar att stå i strid med lag eller annan författning.

Korrigerande befogenheter

4 § Om tillsynsmyndigheten konstaterar att personuppgifter behandlas i strid med lag eller annan författning, eller att Försvarsmakten eller ett personuppgiftsbiträde annars inte fullgör sina skyldigheter, får tillsynsmyndigheten

1. genom sådana åtgärder som anges i 3 § första stycket försöka förmå Försvarsmakten eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsenlig eller att uppfylla andra skyldigheter, eller
2. förelägga Försvarsmakten eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsenlig eller att fullgöra andra skyldigheter.

Om ett föreläggande utfärdas ska det av föreläggandet framgå när åtgärderna senast ska vara genomförda och, om det är lämpligt, vilka åtgärder som ska vidtas.

7 kap. Skadestånd och överklagande

Skadestånd

1 § Den personuppgiftsansvarige ska ersätta den som personuppgiften rör för skada och kränkning av den personliga integriteten som orsakats av behandling av personuppgifter i strid med denna lag, eller föreskrifter som har meddelats i anslutning till den.

Ersättningsskyldigheten kan i den utsträckning det är skäligt, jämkas om den personuppgiftsansvarige visar att felet inte berodde på denne.

Överklagande

2 § Försvarsmaktens beslut om information som ska lämnas enligt 5 kap. 2 och 3 §§ och om rättelse och underrättelse till tredje part enligt 5 kap. 6 § får överklagas hos allmän förvaltningsdomstol. Andra beslut enligt denna lag får inte överklagas.

Prövningstillstånd krävs vid överklagande till kammarrätten.

3 § Av 6 kap. 8 § offentlighets- och sekretesslagen (2009:400) följer att beslut om sekretess överklagas till kammarrätt.

---

1. Denna lag träder i kraft den 1 oktober 2019.

2. Bestämmelsen i 4 kap. 2 § om loggning behöver inte tillämpas på automatiserade system för behandling av personuppgifter som inrättats före ikraftträdandet förrän den 1 maj 2024.

3. Ärenden om tillsyn eller granskning av Försvarsmaktens personuppgiftsbehandling som Datainspektionen eller Statens inspektion för försvarsunderrättelseverksamheten inte har avgjort före ikraftträdandet handläggs enligt äldre föreskrifter.

1.2 Förslag till lag (2019:000) om behandling av personuppgifter vid Försvarets radioanstalt

Härigenom föreskrivs följande.

1 kap. Allmänna bestämmelser

Syftet med lagen

1 § Syftet med denna lag är att säkerställa att Försvarets radioanstalt kan behandla personuppgifter på ett ändamålsenligt sätt och att skydda fysiska personers grundläggande fri- och rättigheter i samband med sådan behandling.

Lagens tillämpningsområde

2 § Denna lag gäller vid behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet samt informationssäkerhetsverksamhet.

3 § Lagen gäller vid sådan behandling av personuppgifter som 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.

4 § Vid behandling av personuppgifter enligt denna lag gäller inte lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

Förhållandet till annan reglering

5 § Bestämmelserna i denna lag ska inte tillämpas i den utsträckning det skulle inskränka skyldigheten enligt 2 kap. tryckfrihetsförordningen att lämna ut personuppgifter.

Personuppgiftsansvar

6 § Försvarets radioanstalt är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför.

Personuppgiftsansvaret omfattar all behandling av personuppgifter som utförs under myndighetens ledning eller på dess vägnar.

7 § Försvarets radioanstalt får vara gemensamt personuppgiftsansvarig med annan endast i den utsträckning det följer av lag eller förordning eller om regeringen i ett enskilt fall beslutar om det.

Definitioner

8 § I denna lag används följande uttryck med nedan angiven betydelse.

Uttryck	*Betydelse*
Behandling av personuppgifter	En åtgärd eller kombination av åtgärder som vidtas i fråga om personuppgifter eller uppsättningar av personuppgifter, oavsett om det görs automatiserat eller inte, t.ex. insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämnande, spridning eller tillhandahållande på annat sätt, justering, sammanföring, begränsning, radering eller förstöring.
Biometriska uppgifter	Personuppgifter som rör en persons fysiska, fysiologiska eller beteendemässiga kännetecken, som tagits fram genom särskild

	teknisk behandling och som möjliggör eller bekräftar unik identifiering av personen i fråga.
Dataskyddsombud	En fysisk person som utses av den personuppgiftsansvarige för att självständigt se till att personuppgifter behandlas författningsenligt och på ett korrekt sätt.
Genetiska uppgifter	Personuppgifter som rör en persons nedärvda eller förvärvade genetiska kännetecken och som härrör från analys av ett spår av eller ett prov från personen i fråga.
Logg	Behandlingshistorik som sparas viss tid.
Mottagare	Den till vilken personuppgifter lämnas ut, med undantag av en myndighet som med stöd av författning utövar tillsyn, kontroll eller revision.
Personuppgift	Varje upplysning om en identifierad eller identifierbar fysisk person som är i livet.
Personuppgiftsansvarig	Den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter.

Personuppgiftsbiträde	Den som, med stöd av ett skriftligt avtal eller annan skriftlig överenskommelse, behandlar personuppgifter för den personuppgiftsansvariges räkning.
Tredje part	Någon annan än den som personuppgiften rör, personuppgiftsansvarige, dataskyddsombudet, personuppgiftsbiträdet och sådana personer som under den personuppgiftsansvariges eller personuppgiftsbiträdets direkta ansvar har rätt att behandla personuppgifter.
Uppgiftssamling	En samling med uppgifter som med hjälp av automatiserad behandling är gemensamt tillgängliga.

2 kap. Behandling av personuppgifter

Rättsliga grunder

Försvarsunderrättelseverksamhet

1 § Personuppgifter får behandlas i Försvarets radioanstalts försvarsunderrättelseverksamhet om det är nödvändigt för att bedriva den verksamhet som anges i lagen (2000:130) om försvarsunderrättelseverksamhet och lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet.

2 § De personuppgifter som Försvarets radioanstalt har fått tillgång till i myndighetens försvarsunderrättelseverksamhet får fortsatt behandlas i den verksamheten, om det behövs för att fullgöra den.

Vad som sägs i första stycket gäller endast om inget annat följer av denna lag eller förordning som regeringen har meddelat i anslutning till lagen.

3 § Personuppgifter som behandlas med stöd av 1 och 2 §§ får även behandlas om det är nödvändigt för att tillhandahålla information som behövs

1. i verksamhet hos berörda myndigheter som avses i 2 § första stycket lagen (2000:130) om försvarsunderrättelseverksamhet,
2. med anledning av samarbete med andra länder och internationella organisationer enligt lagen (2000:130) om försvarsunderrättelseverksamhet och lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet,
3. i utvecklingsverksamheten för de ändamål som anges i 4 §,
4. i informationssäkerhetsverksamheten för de ändamål som anges i 6 §, eller
5. för att biträda andra myndigheter i den utsträckning det följer av lag eller förordning eller om regeringen i ett enskilt fall beslutar om det.

Utvecklingsverksamhet

4 § Om det är nödvändigt för försvarsunderrättelseverksamheten får Försvarets radioanstalt behandla personuppgifter för att

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

5 § Personuppgifter som behandlas med stöd av 4 § får även behandlas om det är nödvändigt för att tillhandahålla information som behövs

1. med anledning av samverkan med annan avseende utvecklingsverksamhet,
2. med anledning av samarbete om utvecklingsverksamhet med andra länder eller internationella organisationer enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet,
3. i försvarsunderrättelseverksamheten för de ändamål som anges i 1 och 2 §§,
4. i informationssäkerhetsverksamhet för de ändamål som anges i 6 §, eller

5. för att biträda andra myndigheter i den utsträckning det följer av lag eller förordning eller om regeringen i ett enskilt fall beslutar om det.

Informationssäkerhetsverksamhet

6 § Personuppgifter får behandlas i Försvarets radioanstalts informationssäkerhetsverksamhet om det är nödvändigt för att kunna skydda den egna myndigheten eller för att kunna stödja andra verksamheter som är av betydelse för Sveriges säkerhet. Uppgiften att lämna stöd till andra verksamheter ska följa av lag eller förordning eller regeringsbeslut i ett enskilt fall.

7 § Personuppgifter som behandlas med stöd av 6 § får även behandlas om det är nödvändigt för att tillhandahålla information som behövs

1. i verksamhet hos den som tar emot uppgifter om informationssäkerhet,
2. med anledning av samverkan med andra som verkar på informationssäkerhetsområdet såväl inom som utom landet i den utsträckning det följer av lag eller förordning eller om regeringen i ett enskilt fall beslutar om det,
3. i försvarsunderrättelseverksamheten för de ändamål som anges i 1 § andra stycket 5 och 7 lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet, eller
4. i utvecklingsverksamheten för de ändamål som anges i 4 §.

Övriga rättsliga grunder

8 § Personuppgifter som utgör allmänt tillgänglig information får behandlas av Försvarets radioanstalt om det är nödvändigt för de ändamål som anges i 1, 2, 4 och 6 §§.

9 § Försvarets radioanstalt får behandla personuppgifter för vetenskapliga, statistiska eller historiska ändamål inom denna lags tillämpningsområde.

10 § Försvarets radioanstalt får behandla personuppgifter för att kunna tillgodose enskildas behov av information enligt 5 kap. och kunna lämna information vid tillsyn eller kontroll.

Grundläggande krav

Ändamål

11 § Personuppgifter får bara behandlas för särskilda, uttryckligt angivna och berättigade ändamål.

Personuppgifter får inte behandlas för något ändamål som är oförenligt med det ändamål för vilket personuppgifterna ursprungligen behandlades.

Författningsenlig och korrekt behandling

12 § Personuppgifter ska behandlas författningsenligt och på ett korrekt sätt.

Personuppgifternas kvalitet

13 § Personuppgifter som behandlas ska vara adekvata och relevanta i förhållande till ändamålen med behandlingen och, om det är nödvändigt, uppdaterade.

Uppgifter som beskriver en persons utseende ska utformas på ett objektivt sätt med respekt för människovärdet.

Fler personuppgifter får inte behandlas än vad som är nödvändigt med hänsyn till ändamålen med behandlingen.

Känsliga personuppgifter

14 § Personuppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening eller som rör hälsa, sexualliv eller sexuell läggning får inte behandlas.

När uppgifter om en person behandlas får de dock kompletteras med sådana uppgifter som avses i första stycket, om det är absolut nödvändigt för syftet med behandlingen.

15 § Biometriska uppgifter får behandlas endast om det är absolut nödvändigt för ändamålet för behandlingen. Genetiska uppgifter får inte behandlas.

16 § Vid sökning får personuppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening eller som rör hälsa, sexualliv eller sexuell läggning användas som sökbegrepp om det är absolut nödvändigt för syftet med behandlingen. Detsamma gäller biometriska uppgifter.

Om den som uppgifterna rör har offentliggjort uppgifterna

17 § Utan hinder av vad som föreskrivs i 14 och 15 §§ får personuppgifter behandlas, om den som personuppgifterna rör på ett tydligt sätt offentliggjort uppgifterna.

Första stycket gäller inte genetiska uppgifter.

Behandling av personuppgifter i vissa fall

18 § Hantering av information som innebär behandling av personuppgifter ska inte anses oförenlig med bestämmelserna i 1, 4, 6, 8 och 11–15 §§ i det skede av behandlingen då det inte har kunnat fastställas vilka personuppgifter som informationen innehåller.

Längsta tid som personuppgifter får behandlas

19 § Personuppgifter som behandlas automatiserat får inte behandlas under längre tid än vad som behövs för något eller några av de ändamål som anges i 1–10 §§.

Regeringen eller den myndighet regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter eller i ett enskilt fall besluta att personuppgifter får behandlas under endast

viss tid eller bevaras för historiska, statistiska eller vetenskapliga ändamål.

Utlämnande av personuppgifter

20 § Personuppgifter som behandlas med stöd av denna lag får föras över till en utländsk underrättelse- eller säkerhetstjänst, en utländsk organisation inom informationssäkerhetsområdet eller en internationell organisation endast om sekretess inte hindrar det och det är nödvändigt för att Försvarets radioanstalt ska kunna fullgöra sina uppgifter inom ramen för internationellt försvarsunderrättelse- och säkerhetssamarbete.

Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter eller i enskilt fall besluta att överföring får ske även i andra fall då det är nödvändigt för verksamheten vid Försvarets radioanstalt.

21 § Personuppgifter får lämnas ut elektroniskt på annat sätt än genom direktåtkomst om regeringen har meddelat föreskrifter eller särskilt beslutat om det.

Elektroniskt utlämnande genom direktåtkomst är tillåtet bara i den utsträckning som anges i 3 kap. 2–6 §§.

3 kap. Gemensamt tillgängliga uppgifter

Personuppgifter som får göras gemensamt tillgängliga

1 § Personuppgifter får göras gemensamt tillgängliga och behandlas i uppgiftssamlingar om det behövs för något av de ändamål som anges i 2 kap. 1–10 §§. Personuppgifter som endast ett fåtal personer har tillgång till anses inte som gemensamt tillgängliga.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter eller besluta i enskilda fall vilka uppgiftssamlingar som får finnas och vilka uppgifter som får behandlas i respektive uppgiftssamling.

Direktåtkomst

Försvarsunderrättelseverksamhet

2 § Trots sekretess enligt 38 kap. 4 § offentlighets- och sekretesslagen (2009:400) får Säkerhetspolisen och Försvarsmakten medges direktåtkomst till personuppgifter som utgör analysresultat inom försvarsunderrättelseverksamheten och som finns i uppgiftssamlingar.

3 § Om det behövs för samarbetet mot terrorism eller för annat internationellt säkerhetssamarbete får, i den utsträckning det följer av lag eller förordning eller om regeringen i ett enskilt fall beslutar om det, en utländsk underrättelse- eller säkerhetstjänst medges direktåtkomst till personuppgifter som behandlas med stöd av 2 kap. 1 § och som finns i uppgiftssamlingar.

Informationssäkerhetsverksamhet

4 § Om det behövs för samarbetet mot it-relaterade hot mot samhällsviktiga system får, i den utsträckning det följer av lag eller förordning eller om regeringen i ett enskilt fall beslutar om det, en utländsk organisation inom informationssäkerhetsområdet medges direktåtkomst till personuppgifter som behandlas med stöd av 2 kap. 6 § och som finns i uppgiftssamlingar.

Direktåtkomst i andra fall

5 § Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter eller särskilt beslut om vilka som i andra fall än i 2–4 §§ får ha direktåtkomst till uppgiftssamlingar.

Övriga bestämmelser

6 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela

1. ytterligare föreskrifter eller beslut i enskilda fall om omfattningen av direktåtkomsten, och
2. föreskrifter om behörighet och säkerhet vid sådan åtkomst.

4 kap. Skyldighet som personuppgiftsansvarig

Åtgärder för att säkerställa författningsenlig behandling

1 § Försvarets radioanstalt ska, genom lämpliga tekniska och organisatoriska åtgärder, säkerställa att behandlingen av personuppgifter är författningsenlig och skydda rättigheterna för dem som uppgifterna rör.

2 § Försvarets radioanstalt ska säkerställa att det i uppgiftsamlingar förs loggar över personuppgiftsbehandling. Regeringen eller den myndighet regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om loggar.

3 § Tillgången till personuppgifter ska alltid begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter.

Säkerheten för personuppgifter

4 § Försvarets radioanstalt ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas, särskilt mot obehörig eller otillåten behandling eller förstöring och mot förlust eller annan oavsiktlig skada.

Dataskyddsombud

5 § Försvarets radioanstalt ska inom myndigheten utse ett eller flera dataskyddsombud och anmäla dessa till tillsynsmyndigheten när dataskyddsombud utses och entledigas.

6 § Dataskyddsombudet ska

1. självständigt kontrollera att Försvarets radioanstalt behandlar personuppgifter författningsenligt och på ett korrekt sätt och i övrigt fullgör sina skyldigheter,
2. informera och ge råd till Försvarets radioanstalt och till dem som behandlar personuppgifter under myndighetens ledning om deras skyldigheter vid behandling av personuppgifter,
3. samråda med tillsynsmyndigheten, och

4. föra en förteckning över de kategorier av behandlingar som Försvarets radioanstalt ansvarar för och som är helt eller delvis automatiserade.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om vad en förteckning som avses i första stycket 4 ska innehålla.

Om Försvarets radioanstalt bryter mot de bestämmelser som gäller för behandlingen av personuppgifter och rättelse inte vidtas, ska dataskyddsombudet anmäla det till tillsynsmyndigheten.

Personuppgiftsbiträden

7 § Försvarets radioanstalt får, om det är lämpligt, anlita personuppgiftsbiträden för behandling av personuppgifter på Försvarets radioanstalts vägnar. Innan ett personuppgiftsbiträde anlitas, ska Försvarets radioanstalt försäkra sig om att biträdet kommer att vidta de lämpliga tekniska och organisatoriska åtgärder som krävs för att behandlingen av personuppgifter ska vara författningsenlig och för att skydda rättigheterna för den som uppgifterna rör.

8 § Personuppgiftsbiträdets behandling av personuppgifter ska regleras i ett skriftligt avtal eller annan skriftlig överenskommelse.

9 § Ett personuppgiftsbiträde får inte anlita ett annat personuppgiftsbiträde utan skriftligt tillstånd av Försvarets radioanstalt.

10 § Ett personuppgiftsbiträde eller den eller de personer som arbetar under biträdets eller Försvarets radioanstalts ledning ska behandla personuppgifter i enlighet med instruktioner från Försvarets radioanstalt.

Om ett personuppgiftsbiträde, i strid med Försvarets radioanstalts instruktioner, bestämmer ändamålen med och medlen för behandlingen, ska biträdet anses vara personuppgiftsansvarig enligt denna lag för den behandlingen.

11 § Det som sägs om Försvarets radioanstalts skyldigheter i 2–4 §§ gäller även för personuppgiftsbiträden som Försvarets radioanstalt anlitar.

5 kap. Enskildas rättigheter

Rätten till information

Allmän information

1 § Försvarets radioanstalt ska göra följande allmänna information tillgänglig.

1. Myndighetens identitet och kontaktuppgifter.
2. Uppgifter om dataskyddsombudet.
3. Ändamålen med behandlingen.
4. Rätten enligt 2 § att begära att få information om behandling av personuppgifter och att få del av dem.
5. Rätten att begära rättelse, radering eller begränsning av behandlingen enligt 5 §.

Information som ska lämnas efter begäran

2 § Försvarets radioanstalt är skyldig att utan onödigt dröjsmål en gång per kalenderår till den som begär det lämna skriftligt besked om personuppgifter som rör honom eller henne behandlas. Behandlas sådana uppgifter ska sökanden få del av dem och få följande skriftliga information.

1. Vilka personuppgifter om den sökande som behandlas.
2. Varifrån personuppgifterna kommer.
3. Den rättsliga grunden för behandlingen.
4. Ändamålen med behandlingen.
5. Mottagare eller kategorier av mottagare av personuppgifterna, även i annat land eller internationella organisationer.
6. Hur länge personuppgifterna får behandlas eller, om det inte är möjligt att ange, kriterierna för att fastställa det.
7. Rätten att begära rättelse, radering eller begränsning av behandlingen enligt 5 §.

Utlämnande enligt första stycket behöver inte omfatta personuppgifter som sökanden har tagit del av, om inte han eller hon begär det. Det ska dock framgå av informationen att personuppgifterna i fråga behandlas.

En ansökan enligt första stycket ska göras skriftligen hos Försvarets radioanstalt och vara undertecknad av den sökande själv. Information enligt första stycket ska 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.

Begränsning av rätten till information

3 § Informationsskyldigheten i 2 § gäller inte i den utsträckning sekretess hindrar att uppgifterna lämnas ut.

Om förutsättningarna i första stycket är uppfyllda, är Försvarets radioanstalt inte skyldig att lämna ut skälen för beslut enligt första stycket eller beslut i fråga om rättelse, radering eller begränsning av behandlingen enligt 5 §.

4 § Informationsskyldigheten i 2 § gäller inte personuppgifter i löpande text som inte fått sin slutliga utformning när begäran gjordes eller som utgör minnesanteckning eller liknande.

Informationsskyldigheten gäller dock om uppgifterna har lämnats ut till tredje part, behandlas enbart för vetenskapliga, statistiska eller historiska ändamål eller arkivändamål av allmänt intresse eller, när det gäller löpande text som inte fått sin slutliga utformning, om uppgifterna har behandlats längre än ett år.

Rätten till rättelse, radering och begränsning av behandlingen

5 § Försvarets radioanstalt ska på begäran av den som personuppgiften rör snarast rätta, radera eller begränsa sådana personuppgifter som inte har behandlats i enlighet med denna lag eller föreskrifter som har meddelats med stöd av lagen.

Försvarets radioanstalt ska också underrätta tredje part till vilken uppgifterna har lämnats ut om åtgärden, om den som personuppgiften rör begär det eller om en mera betydande skada eller olägenhet för denne skulle kunna undvikas genom en underrättelse.

Någon underrättelse behöver dock inte lämnas, om sekretess hindrar det eller detta är omöjligt eller skulle innebära en oproportionerligt stor arbetsinsats.

Avgiftsfri information

6 § Information enligt 1 § ska lämnas utan avgift.

Information och uppgifter enligt 2 § ska lämnas utan avgift en gång per kalenderår. Om någon begär information och uppgifter enligt 2 § oftare än en gång per kalenderår, får Försvarets radioanstalt avslå begäran.

6 kap. Tillsyn

Tillsyn över personuppgiftsbehandlingen

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

Tillsynsmyndigheten ska ge råd och stöd till Försvarets radioanstalt om myndighetens skyldigheter enligt lag eller annan författning eller när det i övrigt är påkallat.

2 § I lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet finns det särskilda bestämmelser om kontroll som rör Försvarets radioanstalts behandling av personuppgifter i försvarsunderrättelse- och utvecklingsverksamheten.

Befogenheter

Utredningsbefogenheter

3 § Tillsynsmyndigheten har rätt att av Försvarets radioanstalt eller ett personuppgiftsbiträde på begäran få

1. tillgång till personuppgifter som behandlas,
2. upplysningar om och dokumentation av behandlingen av personuppgifter och säkerhets- och skyddsåtgärder,
3. tillträde till sådana lokaler som har anknytning till behandling av personuppgifter och tillgång till utrustning och andra medel för behandling av personuppgifter, och
4. det biträde och annan information som behövs för tillsynen.

Förebyggande befogenheter

4 § Om tillsynsmyndigheten bedömer att det finns risk för att personuppgifter kan komma att behandlas i strid med lag eller annan författning, ska myndigheten genom råd, rekommendationer eller påpekanden försöka förmå Försvarets radioanstalt eller personuppgiftsbiträdet att vidta åtgärder för att minska den risken.

Tillsynsmyndigheten får utfärda en skriftlig varning för att planerad behandling av personuppgifter riskerar att stå i strid med lag eller annan författning. Detsamma gäller om pågående behandling riskerar att stå i strid med lag eller annan författning.

Korrigerande befogenheter

5 § Om tillsynsmyndigheten konstaterar att personuppgifter behandlas i strid med lag eller annan författning, eller att Försvarets radioanstalt eller ett personuppgiftsbiträde annars inte fullgör sina skyldigheter, får tillsynsmyndigheten

1. genom sådana åtgärder som anges i 4 § första stycket försöka förmå Försvarets radioanstalt eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsenlig eller att uppfylla andra skyldigheter, eller
2. förelägga Försvarets radioanstalt eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsenlig eller att fullgöra andra skyldigheter.

Om ett föreläggande utfärdas ska det av föreläggandet framgå när åtgärderna senast ska vara genomförda och, om det är lämpligt, vilka åtgärder som ska vidtas.

7 kap. Skadestånd och överklagande

Skadestånd

1 § Den personuppgiftsansvarige ska ersätta den som personuppgiften rör för skada och kränkning av den personliga integriteten som orsakats av behandling av personuppgifter i strid med denna lag, eller föreskrifter som har meddelats i anslutning till den.

Ersättningsskyldigheten kan i den utsträckning det är skäligt, jämkas om den personuppgiftsansvarige visar att felet inte berodde på denne.

Överklagande

2 § Försvarets radioanstalts beslut om information som ska lämnas enligt 5 kap. 2 § och om rättelse och underrättelse till tredje part enligt 5 kap. 5 § får överklagas hos allmän förvaltningsdomstol. Andra beslut enligt denna lag får inte överklagas.

Prövningstillstånd krävs vid överklagande till kammarrätten.

3 § Av 6 kap. 8 § offentlighets- och sekretesslagen (2009:400) följer att beslut om sekretess överklagas till kammarrätt.

---

1. Denna lag träder i kraft den 1 oktober 2019.

2. Bestämmelsen i 4 kap. 2 § om loggning behöver inte tillämpas på uppgiftssamlingar som inrättats före ikraftträdandet förrän den 1 maj 2024.

3. Ärenden om tillsyn eller granskning av Försvarets radioanstalts personuppgiftsbehandling som Datainspektionen eller Statens inspektion för försvarsunderrättelseverksamheten inte har avgjort före ikraftträdandet handläggs enligt äldre föreskrifter.

1.3 Förslag till lag om ändring i lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning

Härigenom föreskrivs att 1 kap. 3 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	1 kap.
	3 §
Bestämmelserna i 2 § gäller inte i verksamhet som omfattas av	
1. *lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst,*	1. *lagen (2019:000) om behandling av personuppgifter vid Försvarsmakten*,
2. *lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet*, eller	2. *lagen (2019:000) om behandling av personuppgifter vid Försvarets radioanstalt*, eller
3. 6 kap. polisdatalagen (2010:361).	3. 6 kap. polisdatalagen (2010:361).

Denna lag träder i kraft den 1 oktober 2019.

1.4 Förslag till lag om ändring i lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet

Härigenom föreskrivs att 2 a och 12 a §§ lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet ska ha följande lydelser.

Nuvarande lydelse	*Föreslagen lydelse*
	2 a §
Inhämtning får inte avse signaler mellan en avsändare och mottagare som båda befinner sig i Sverige. Om sådana signaler inte kan avskiljas redan vid inhämtningen, ska upptagningen eller upptecknningen förstöras så snart det står klart att sådana signaler har inhämtats.	
Första stycket tillämpas inte i fråga om signaler mellan sändare och mottagare på utländska statsfartyg, statsluftfartyg eller militära fordon.	Första stycket tillämpas inte i fråga om signaler *som utväxlas autonomt mellan tekniska system i sådana fall där signalerna inte innehåller personuppgifter. Första stycket tillämpas inte heller i fråga om övriga* signaler mellan sändare och mottagare på utländska statsfartyg, statsluftfartyg eller militära fordon.
	12 a §
I lagen *(2007:259)* om behandling av personuppgifter *i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet* finns ytterligare bestämmelser om behandlingen av inhämtade personuppgifter.	I lagen *(2019:000)* om behandling av personuppgifter *vid Försvarets radioanstalt* finns ytterligare bestämmelser om behandlingen av inhämtade personuppgifter.

Denna lag träder i kraft den 1 oktober 2019.

1.5 Förslag till lag om ändring i brottsdatalagen (2018:1177)

Härigenom föreskrivs att 1 kap. 4 § brottsdatalagen (2018:1177) ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	1 kap.
	4 §
	Lagen gäller inte vid Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet eller om Polismyndigheten har övertagit en arbetsuppgift som rör nationell säkerhet från Säkerhetspolisen.
Lagen gäller inte heller i sådan verksamhet som omfattas av *lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst.*	Lagen gäller inte heller i sådan verksamhet som omfattas av *lagen (2019:000) om behandling av personuppgifter vid Försvarsmakten.*

Denna lag träder i kraft den 1 oktober 2019.

1.6 Förslag till förordning (2019:000) om behandling av personuppgifter vid Försvarsmakten

Härigenom föreskrivs följande.

1 kap. Allmänna bestämmelser

Syfte

1 § I denna förordning finns kompletterande föreskrifter till lagen (2019:000) om behandling av personuppgifter vid Försvarsmakten. Uttryck som används i förordningen har samma innebörd som i den lagen.

Gemensamt personuppgiftsansvar

2 § Försvarsmakten får vara gemensamt personuppgiftsansvarig med Säkerhetspolisen, Nationella operativa avdelningen i Polismyndigheten, Myndigheten för samhällsskydd och beredskap, Försvarets materielverk, Försvarets radioanstalt och Totalförsvarets rekryteringsmyndighet.

3 § När Försvarsmakten är gemensamt personuppgiftsansvarig med annan ska myndigheten säkerställa att de förpliktelser var och en har i egenskap av personuppgiftsansvarig regleras i en skriftlig överenskommelse. Vid sådan överenskommelse kvarstår Försvarsmaktens författningsenliga skyldigheter.

Den som personuppgiften rör får, trots en sådan överenskommelse som avses i första stycket, utöva sina rättigheter gentemot var och en av de personuppgiftsansvariga.

2 kap. Behandling av personuppgifter

Utlämnande av personuppgifter

1 § Säkerhetspolisen, Polismyndigheten, Myndigheten för samhällsskydd och beredskap, Migrationsverket, Försvarets materielverk, Försvarets radioanstalt, Totalförsvarets forskningsinstitut, Totalförsvarets rekryteringsmyndighet, Fortifikationsverket och Försvarshögskolan har rätt att vid direktåtkomst enligt 3 kap. 6, 7, 9 och 10 §§ ta del av de personuppgifter som omfattas av åtkomsten.

2 § Försvarsmakten får inom ramen för internationellt försvars- och säkerhetssamarbete överföra personuppgifter till en utländsk myndighet eller en internationell organisation, om överföringen tjänar den svenska statsledningen eller det svenska totalförsvaret.

Överföringen av personuppgifter enligt första stycket får inte vara till skada för svenska intressen.

3 kap. Gemensamt tillgängliga uppgifter

Uppgiftssamlingar

Försvarsunderrättelseverksamhet

1 § Vid Försvarsmakten får det finnas uppgiftssamlingar för försvarsunderrättelseverksamhet som innehåller personuppgifter. Uppgiftssamlingarna får endast innehålla uppgifter som är nödvändiga för att Försvarsmakten ska kunna bedriva verksamhet enligt lagen (2000:130) om försvarsunderrättelseverksamhet.

2 § En uppgiftssamling för försvarsunderrättelseverksamhet får endast innehålla

1. identifieringsuppgifter,
2. uppgifter om de omständigheter och händelser som ger anledning att anta att den som behandlingen rör har betydelse för försvarsunderrättelseverksamheten,
3. upplysningar om varifrån uppgiften kommer och om en uppgiftslämnares trovärdighet, och
4. allmänt tillgänglig information som finns på internet eller i öppna databaser.

När personuppgifter som avses i första stycket och som finns i rapportunderlag och underrättelserapporter inte längre behövs för de ändamål för vilka de behandlas, ska de bevaras för historiska, statistiska eller vetenskapliga ändamål.

Militär säkerhetstjänst

3 § Vid Försvarsmakten får det finnas uppgiftssamlingar för säkerhetsunderrättelsetjänst som innehåller personuppgifter. Uppgiftssamlingarna får endast innehålla uppgifter som är nödvändiga för att upptäcka och klarlägga säkerhetshotande verksamhet som riktas mot Försvarsmakten och dess säkerhetsintressen samt allmänt tillgänglig information som finns på internet eller i öppna databaser.

När personuppgifter som avses i första stycket och som finns i rapportunderlag och underrättelserapporter inte längre behövs för de ändamål för vilka de behandlas, ska de bevaras för historiska, statistiska eller vetenskapliga ändamål.

4 § Vid Försvarsmakten får det finnas uppgiftssamlingar för säkerhetsskyddstjänst som innehåller personuppgifter. Uppgiftssamlingarna får endast innehålla uppgifter som är nödvändiga för att förebygga och avvärja säkerhetshotande verksamhet som riktas mot Försvarsmakten och dess säkerhetsintressen.

5 § Vid Försvarsmakten får det finnas uppgiftssamlingar för signalkontroll som innehåller personuppgifter. Uppgiftssamlingarna får endast innehålla uppgifter som är nödvändiga för att förhindra obehörig insyn i och påverkan av totalförsvarets telekommunikations- och informationssystem.

Personuppgifter i en uppgiftssamling för signalkontroll får inte behandlas längre än ett år efter att behandlingen av uppgifterna påbörjades.

Övrig verksamhet

6 § För sådan verksamhet som inte utgör försvarsunderrättelseverksamhet eller militär säkerhetstjänst får Försvarsmakten bestämma vilka uppgiftssamlingar myndigheten ska ha och vad de ska innehålla.

Direktåtkomst

Försvar och säkerhet

7 § Försvarets materielverk får medges direktåtkomst till personuppgifter som behandlas med stöd av 2 kap. 1 § lagen (2019:000) om behandling av personuppgifter vid Försvarsmakten. Direktåtkomsten får endast avse personuppgifter som rör Försvarsmaktens materiel- och logistikförsörjning och som har gjorts gemensamt tillgängliga.

8 § Totalförsvarets rekryteringsmyndighet får medges direktåtkomst till personuppgifter om som behandlas med stöd av 2 kap. 1 § lagen (2019:000) om behandling av personuppgifter vid Försvarsmakten. Direktåtkomsten får endast avse personuppgifter som rör totalförsvarspliktiga och Försvarsmaktens krigsorganisation och som har gjorts gemensamt tillgängliga.

9 § Finlands försvarsmakt får medges direktåtkomst till personuppgifter som behandlas med stöd av 2 kap. 1 § lagen (2019:000) om behandling av personuppgifter vid Försvarsmakten om det behövs för planering, förberedelser och genomförande av stöd inom ramen för lagen (2019:000) om operativt militärt stöd mellan Sverige och Finland. Direktåtkomsten får endast avse personuppgifter som har gjorts gemensamt tillgängliga.

Försvarsunderrättelseverksamhet

10 § Regeringskansliet, Säkerhetspolisen, Nationella operativa avdelningen i Polismyndigheten, Myndigheten för samhällsskydd och beredskap, Inspektionen för strategiska produkter, Försvarets materielverk, Totalförsvarets forskningsinstitut och Tullverket får medges direktåtkomst till personuppgifter som utgör analysresultat och

underrättelser och som finns i uppgiftssamlingar för försvarsunderrättelseverksamhet.

11 § Om det behövs för samarbetet mot terrorism eller vid svenskt deltagande i annat internationellt underrättelse- och säkerhetssamarbete får en utländsk underrättelse- eller säkerhetstjänst medges direktåtkomst till personuppgifter som behandlas enligt 2 kap. 2 § lagen (2019:000) om behandling av personuppgifter vid Försvarsmakten och som finns i en uppgiftssamling som Försvarsmakten upprättat i syfte att dela informationen med mottagaren.

Innan direktåtkomst medges en utländsk underrättelse- eller säkerhetstjänst enligt första stycket ska Försvarsmakten underrätta Regeringskansliet (Försvarsdepartementet).

Militär säkerhetstjänst

12 § Säkerhetspolisen, Nationella operativa avdelningen i Polismyndigheten, Myndigheten för samhällsskydd och beredskap, Migrationsverket, Försvarets materielverk, Försvarets radioanstalt, Totalförsvarets forskningsinstitut, Totalförsvarets rekryteringsmyndighet, Fortifikationsverket och Försvarshögskolan får medges direktåtkomst till personuppgifter som behandlas med stöd av 2 kap. 5 § första stycket 1 och 2 lagen (2019:000) om behandling av personuppgifter vid Försvarsmakten och som finns i en uppgiftssamling för säkerhetsunderrättelsetjänst.

13 § Säkerhetspolisen får medges direktåtkomst till personuppgifter som behandlas med stöd av 2 kap. 5 § första stycket 5 lagen (2019:000) om behandling av personuppgifter vid Försvarsmakten och som finns i en uppgiftssamling för säkerhetsskyddstjänst.

14 § Om det behövs för samarbetet mot säkerhetshotande verksamhet som riktas mot Försvarsmakten och dess säkerhetsintressen får en utländsk underrättelse- eller säkerhetstjänst medges direktåtkomst till personuppgifter som behandlas med stöd av 2 kap. 5 § 1 och 2 och som finns i en avskild uppgiftssamling som Försvarsmakten upprättat i syfte att dela informationen med mottagaren.

Innan direktåtkomst medges en utländsk underrättelse- eller säkerhetstjänst enligt första stycket ska Försvarsmakten underrätta Regeringskansliet (Försvarsdepartementet).

Omfattning av direktåtkomst

15 § Försvarsmakten beslutar om omfattningen av direktåtkomst som följer av lag, förordning eller regeringens beslut i enskilt fall.

16 § Försvarsmakten ska säkerställa att förutsättningarna för direktåtkomsten dokumenteras.

Tillgången till uppgifter hos mottagaren ska vara förbehållen de personer som på grund av sina arbetsuppgifter behöver ha tillgång till uppgifterna.

Direktåtkomst får inte medges innan Försvarsmakten har försäkrat sig om att mottagaren uppfyller kraven på behörighet och säkerhet.

4 kap. Skyldigheter som personuppgiftsansvarig

Tekniska och organisatoriska åtgärder

1 § De åtgärder som Försvarsmakten ska vidta enligt 4 kap. 1 § lagen (2019:000) om behandling av personuppgifter vid Försvarsmakten ska vara rimliga med beaktande av behandlingens art, omfattning, sammanhang och ändamål och de särskilda riskerna med behandlingen.

2 § Försvarsmakten ska föra loggar i myndighetens informationssystem som innehåller gemensamt tillgängliga uppgifter. Av loggarna ska framgå vilken medarbetare eller annan som läst, skapat, ändrat eller raderat personuppgifter samt tidpunkten för åtgärden.

Skyldigheten enligt första stycket gäller inte informationssystem som ännu inte börjat användas.

Behörigheter

3 § För tilldelning av behörighet för åtkomst till personuppgifter ska det särskilt beaktas att det, utöver behovet av uppgifterna, ställs krav på utbildning och erfarenhet.

Försvarsmakten ansvarar för att det inom myndigheten finns rutiner för tilldelning, förändring, borttagning och regelbunden uppföljning av behörigheter för åtkomst till personuppgifter.

Säkerheten vid behandling av personuppgifter

4 § Skyddsåtgärder enligt 4 kap. 4 § lagen (2019:000) om behandling av personuppgifter vid Försvarsmakten ska åstadkomma en säkerhetsnivå som är lämplig med beaktande av

1. de tekniska möjligheter som finns,
2. vad det skulle kosta att genomföra åtgärderna,
3. behandlingens art, omfattning, sammanhang och ändamål,
4. de särskilda risker som finns med behandlingen av personuppgifterna,
5. om känsliga personuppgifterna behandlas, och
6. hur integritetskänsliga övriga personuppgifter som behandlas är.

Anmälan av överträdelser

5 § Försvarsmakten ska ha interna rutiner för anmälan av överträdelser av bestämmelser om personuppgiftsbehandling som garanterar att anmälarens identitet skyddas.

Dataskyddsombud

6 § Försvarsmakten ska säkerställa att dataskyddsombud ges möjlighet att delta i de frågor som rör skyddet av personuppgifter.

Försvarsmakten ska se till att dataskyddsombud kan utföra de uppgifter som anges i 4 kap. 6 § lagen (2019:000) om behandling av personuppgifter vid Försvarsmakten genom att tillhandahålla nödvändiga resurser, ge tillgång till dokumentation om behandling av personuppgifter och vid behov medge åtkomst till personuppgifter

som behandlas. Försvarsmakten ska också se till att dataskyddsombud ges möjlighet att upprätthålla sin sakkunskap.

Förteckning över kategorier av behandlingar

7 § Den förteckning över kategorier av behandlingar av personuppgifter som är helt eller delvis automatiserade som ska föras av dataskyddsombudet enligt 4 kap. 6 § första stycket 4 lagen (2019:000) om behandling av personuppgifter vid Försvarsmakten ska innehålla följande uppgifter.

1. Namnet på och kontaktuppgifter till myndigheten.
2. Namnet på och kontaktuppgifter till gemensamt personuppgiftsansvariga.
3. Namnet på dataskyddsombudet.
4. Namnet på personuppgiftsbiträdet.
5. Den rättsliga grunden för behandlingen.
6. Ändamålen med behandlingen.
7. Kategorier av de som berörs av behandlingen.
8. Kategorier av personuppgifter som kan komma att behandlas.
9. Kategorier av tjänstemän som har tillgång till de personuppgifter som behandlas.
10. Säkerhetsåtgärder.
11. Kategorier av mottagare till vilka uppgifterna kan komma att lämnas ut, även i annat land eller internationella organisationer.
12. Överföring av personuppgifter till annat land eller internationella organisationer.

Personuppgiftsbiträden

Avtalets eller överenskommelsens innehåll

8 § Ett avtal eller en annan överenskommelse enligt 4 kap. 8 § lagen (2019:000) om behandling av personuppgifter vid Försvarsmakten ska ange vad behandlingen ska avse, hur länge behandlingen ska pågå, dess art och ändamål, typen av personuppgifter, kategorier av de som berörs av behandlingen och Försvarsmaktens skyldigheter och rättigheter. I avtalet eller överenskommelsen ska det särskilt föreskrivas att personuppgiftsbiträdet ska

1. behandla personuppgifter bara enligt instruktioner från Försvarsmakten,

2. säkerställa att personer som har tillstånd att behandla personuppgifter har förbundit sig att iaktta regler om tystnadsplikt eller omfattas av lagstadgad tystnadsplikt,

3. hjälpa Försvarsmakten att säkerställa att bestämmelserna om de rättigheter som de som behandlingen rör har följts,

4. radera eller återlämna alla personuppgifter till Försvarsmakten när uppdraget har slutförts och, om inte annat följer av lag eller förordning, radera befintliga kopior,

5. ge Försvarsmakten tillgång till den information som krävs för att visa att det som sägs i denna bestämmelse, 9 § och 4 kap. 7, 9–11 §§ lagen (2019:000) om behandling av personuppgifter vid Försvarsmakten följs, och

6. respektera de villkor som framgår av denna bestämmelse och 3 kap. 9 § lagen (2019:000) om behandling av personuppgifter vid Försvarsmakten vid anlitande av ett annat personuppgiftsbiträde.

Övriga skyldigheter

9 § Det som sägs om Försvarsmaktens skyldigheter i 4 § gäller även för personuppgiftsbiträden som Försvarsmakten anlitar.

5 kap. Enskildas rättigheter

Krav på utformningen av information

1 § Information enligt 5 kap. 1–3 §§ lagen (2019:000) om behandling av personuppgifter vid Försvarsmakten ska vara lättillgänglig och lättbegriplig och lämnas i lämplig form.

Beslut

2 § Beslut enligt 5 kap. 3 och 6 §§ lagen (2019:000) om behandling av personuppgifter vid Försvarsmakten ska vara skriftliga. Beslut som går den sökande emot ska motiveras.

Av 5 kap. 4 § andra stycket lagen (2019:000) om behandling av personuppgifter vid Försvarsmakten framgår att skälen för vissa beslut inte behöver lämnas ut.

6 kap. Tillsyn

Tillsynsmyndighet

1 § Datainspektionen är tillsynsmyndighet enligt lagen (2019:000) om behandling av personuppgifter vid Försvarsmakten.

Anmälningsskyldighet

2 § Om Datainspektionen i sin tillsyn uppmärksammar förhållanden som kan utgöra brott, ska myndigheten anmäla det till Åklagarmyndigheten.

Datainspektionen ska samråda med Åklagarmyndigheten innan en sådan anmälan görs. Till anmälan ska inspektionen foga det underlag som finns och även i övrigt lämna det bistånd som behövs i anledning av anmälan.

7 kap. Bemyndiganden

1 § Riksarkivet får, efter samråd med Försvarsmakten, meddela föreskrifter om att personuppgifter som inte längre får behandlas enligt 2 kap. 21 § lagen (2019:000) om behandling av personuppgifter vid Försvarsmakten ska bevaras.

2 § Försvarsmakten får meddela närmare föreskrifter om verkställighet av bestämmelserna i lagen (2019:000) om behandling av personuppgifter vid Försvarsmakten.

Om föreskrifterna berör integritetsskyddet vid personuppgiftsbehandling ska Försvarsmakten samråda med Datainspektionen innan föreskrifterna beslutas.

1. Denna förordning träder i kraft den 1 oktober 2019.

2. Bestämmelserna i 4 kap. 2 § om loggning behöver inte tillämpas på informationssystem som inrättats före ikraftträdandet förrän den 1 maj 2024.

3. Bestämmelserna i 4 kap 7 § om innehållet i förteckningen över kategorier av behandlingar av personuppgifter som är helt eller delvis automatiserade behöver inte tillämpas på de behandlingar av personuppgifter som förtecknats före ikraftträdandet förrän den 1 maj 2024.

1.7 Förslag till förordning (2019:000) om behandling av personuppgifter vid Försvarets radioanstalt

Härigenom föreskrivs följande.

1 kap. Allmänna bestämmelser

Syfte

1 § I denna förordning finns kompletterande föreskrifter till lagen (2019:000) om behandling av personuppgifter vid Försvarets radioanstalt. Uttryck som används i förordningen har samma innebörd som i den lagen.

Gemensamt personuppgiftsansvar

2 § Försvarets radioanstalt får med Försvarsmakten och Säkerhetspolisen ha gemensamt personuppgiftsansvar, inom ramen för myndighetsöverskridande samverkan mellan myndigheterna, för att kunna kartlägga

1. yttre militära hot mot landet,
2. förutsättningar för svenskt deltagande i fredsfrämjande och humanitära internationella insatser eller hot mot säkerheten för svenska intressen vid genomförandet av sådana insatser,
3. strategiska förhållanden avseende internationell terrorism som kan hota väsentliga nationella intressen,
4. allvarliga yttre hot mot samhällets infrastrukturer, eller
5. främmande underrättelseverksamhet mot svenska intressen.

3 § När Försvarets radioanstalt är gemensamt personuppgiftsansvarig med annan ska myndigheten säkerställa att de förpliktelser var och en har i egenskap av personuppgiftsansvarig regleras i en skriftlig överenskommelse. Vid sådan överenskommelse kvarstår Försvarets radioanstalts författningsenliga skyldigheter.

Den som personuppgiften rör får, trots en sådan överenskommelse som avses i första stycket, utöva sina rättigheter gentemot var och en av de personuppgiftsansvariga.

2 kap. Behandling av personuppgifter

Utlämnande av personuppgifter

Överföring av personuppgifter till myndigheter i andra länder och internationella organisationer

1 § Personuppgifter får föras över till en utländsk underrättelse- eller säkerhetstjänst, en utländsk organisation inom informationssäkerhetsområdet eller en internationell organisation, om överföringen tjänar den svenska statsledningen eller det svenska totalförsvaret.

Överföringen av personuppgifter enligt första stycket får inte vara till skada för svenska intressen.

Elektroniskt utlämnande

2 § Personuppgifter får lämnas ut elektroniskt till statliga myndigheter på annat sätt än genom direktåtkomst.

3 kap. Gemensamt tillgängliga uppgifter

Uppgiftssamlingar

Försvarsunderrättelse- och utvecklingsverksamhet

1 § Vid Försvarets radioanstalt får det finnas uppgiftssamlingar för råmaterial som innehåller personuppgifter. Uppgiftssamlingarna får endast innehålla obearbetat och automatiskt bearbetat material vars relevans för verksamheten ännu inte bedömts.

Personuppgifter i en uppgiftssamling för råmaterial får inte behandlas längre än ett år efter det att behandlingen av uppgifterna påbörjades.

2 § Vid Försvarets radioanstalt får det finnas uppgiftssamlingar för analyser som innehåller personuppgifter. Uppgiftssamlingarna får endast innehålla bearbetningsunderlag och analysresultat.

3 § Vid Försvarets radioanstalt får det finnas uppgiftssamlingar för underrättelser som innehåller personuppgifter. Uppgiftssamlingarna får endast innehålla rapportunderlag och färdiga underrättelserapporter.

När personuppgifter i rapportunderlag och underrättelserapporter inte längre behövs för de ändamål för vilka de behandlas ska de bevaras för historiska, statistiska eller vetenskapliga ändamål.

4 § Vid Försvarets radioanstalt får det finnas uppgiftssamlingar för information om signalmiljön som innehåller personuppgifter. Uppgiftssamlingarna får endast innehålla information som rör signalmiljön.

5 § Vid Försvarets radioanstalt får det finnas uppgiftssamlingar för information om företeelser mot vilka signalspaningen inriktas som innehåller personuppgifter. Uppgiftssamlingarna får endast innehålla sådan information om fysiska personer och andra källor som är nödvändig eller kan vara nödvändig för att verkställa inriktningar av signalspaning.

6 § Vid Försvarets radioanstalt får det finnas uppgiftssamlingar för information om teknik- och metodikutveckling som innehåller personuppgifter. Uppgiftssamlingarna får endast innehålla information som rör teknik- och metodikutvecklingen.

7 § Vid Försvarets radioanstalt får det finnas uppgiftssamlingar för signalskydd som innehåller personuppgifter. Uppgiftssamlingarna får endast innehålla information som rör signalskyddet.

Informationssäkerhetsverksamhet

8 § Vid Försvarets radioanstalt får det finnas uppgiftssamlingar för informationssäkerhetsverksamhet som innehåller personuppgifter. Uppgiftssamlingarna får endast innehålla information om uppdragsgivare, information som rör it-angrepp samt bearbetningsunderlag och analysresultat.

Övrigt

9 § Vid Försvarets radioanstalt får det finnas uppgiftssamlingar för allmänt tillgänglig information som innehåller personuppgifter. Uppgiftssamlingarna får endast innehålla information som finns eller har funnits på internet eller i öppna databaser.

10 § Vid Försvarets radioanstalt får det finnas uppgiftsamlingar för loggar som förs med stöd av 2 kap. 10 § och 4 kap. 2 § lagen (2019:000) om behandling av personuppgifter vid Försvarets radioanstalt.

Direktåtkomst

Försvarsunderrättelseverksamhet

11 § Regeringskansliet, Säkerhetspolisen, Nationella operativa avdelningen i Polismyndigheten, Inspektionen för strategiska produkter, Försvarsmakten, Försvarets materielverk, Totalförsvarets forskningsinstitut, Myndigheten för samhällsskydd och beredskap, och Tullverket får medges direktåtkomst till personuppgifter som utgör underrättelser och som finns i uppgiftssamlingar.

Informationssäkerhetsverksamhet

12 § Säkerhetspolisen och Försvarsmakten får medges direktåtkomst till personuppgifter som utgör analysresultat och som behandlas i en uppgiftssamling för informationssäkerhetsverksamhet.

Omfattning av direktåtkomst

13 § Försvarets radioanstalt beslutar om omfattningen av direktåtkomst som följer av lag, förordning eller regeringens beslut i enskilt fall.

14 § Försvarets radioanstalt ska säkerställa att förutsättningarna för direktåtkomsten dokumenteras.

Tillgången till uppgifter hos mottagaren ska vara förbehållen de personer som på grund av sina arbetsuppgifter behöver ha tillgång till uppgifterna.

Direktåtkomst får inte medges innan Försvarets radioanstalt har försäkrat sig om att mottagaren uppfyller kraven på behörighet och säkerhet.

4 kap. Skyldigheter som personuppgiftsansvarig

Tekniska och organisatoriska åtgärder

1 § De åtgärder som Försvarets radioanstalt ska vidta enligt 4 kap. 1, 2 och 4 §§ lagen (2019:000) om behandling av personuppgifter vid Försvarets radioanstalt ska vara rimliga med beaktande av behandlingens art, omfattning, sammanhang och ändamål och de särskilda riskerna med behandlingen.

2 § Försvarets radioanstalt ska föra loggar i myndighetens informationssystem som innehåller uppgiftssamlingar för försvarsunderrättelse- och informationssäkerhetsverksamhet. Av loggarna ska framgå vilken medarbetare eller annan som läst, skapat, ändrat eller raderat personuppgifter samt tidpunkten för åtgärden.

Skyldigheten enligt första stycket gäller inte informationssystem som ännu inte börjat användas.

Behörigheter

3 § För tilldelning av behörighet för åtkomst till personuppgifter ska det särskilt beaktas att det, utöver behovet av uppgifterna, ställs krav på utbildning och erfarenhet.

Försvarets radioanstalt ansvarar för att det inom myndigheten finns rutiner för tilldelning, förändring, borttagning och regelbunden uppföljning av behörigheter för åtkomst till personuppgifter.

Säkerheten vid behandling av personuppgifter

4 § Skyddsåtgärder enligt 4 kap. 4 § lagen (2019:000) om behandling av personuppgifter vid Försvarets radioanstalt ska åstadkomma en säkerhetsnivå som är lämplig med beaktande av

1. de tekniska möjligheter som finns,
2. vad det skulle kosta att genomföra åtgärderna,

3. behandlingens art, omfattning, sammanhang och ändamål,
4. de särskilda risker som finns med behandlingen av personuppgifterna,
5. om känsliga personuppgifterna behandlas, och
6. hur integritetskänsliga övriga personuppgifter som behandlas är.

Anmälan av överträdelser

5 § Försvarets radioanstalt ska ha interna rutiner för anmälan av överträdelser av bestämmelser om personuppgiftsbehandling som garanterar att anmälarens identitet skyddas.

Dataskyddsombud

6 § Försvarets radioanstalt ska säkerställa att dataskyddsombud ges möjlighet att delta i de frågor som rör skyddet av personuppgifter.

Försvarets radioanstalt ska se till att dataskyddsombud kan utföra de uppgifter som anges i 4 kap. 6 § lagen (2019:000) om behandling av personuppgifter vid Försvarets radioanstalt genom att tillhandahålla nödvändiga resurser, ge tillgång till dokumentation om behandling av personuppgifter och vid behov medge åtkomst till personuppgifter som behandlas. Försvarets radioanstalt ska också se till att dataskyddsombud ges möjlighet att upprätthålla sin sakkunskap.

Förteckning över kategorier av behandlingar

7 § Den förteckning över kategorier av behandlingar som ska föras av dataskyddsombudet enligt 4 kap. 6 § första stycket 4 lagen (2019:000) om behandling av personuppgifter vid Försvarets radioanstalt ska innehålla följande uppgifter.

1. Namnet på och kontaktuppgifter till myndigheten.
2. Namnet på och kontaktuppgifter till gemensamt personuppgiftsansvariga.
3. Namnet på dataskyddsombudet.
4. Namnet på personuppgiftsbiträden.
5. Den rättsliga grunden för behandlingen.
6. Ändamålen med behandlingen.

7. Kategorier av de som berörs av behandlingen.

8. Kategorier av personuppgifter som kan komma att behandlas.

9. Kategorier av tjänstemän som har tillgång till de personuppgifter som behandlas.

10. Säkerhetsåtgärder.

11. Kategorier av mottagare till vilka uppgifterna kan komma att lämnas ut, även i annat land eller internationella organisationer.

12. Överföring av personuppgifter till annat land eller internationella organisationer.

Personuppgiftsbiträden

Avtalets eller överenskommelsens innehåll

8 § Ett avtal eller en annan överenskommelse enligt 4 kap. 8 § lagen (2019:000) om behandling av personuppgifter vid Försvarets radioanstalt ska ange vad behandlingen ska avse, hur länge behandlingen ska pågå, dess art och ändamål, typen av personuppgifter, kategorier av de som berörs av behandlingen och Försvarets radioanstalts skyldigheter och rättigheter. I avtalet eller överenskommelsen ska det särskilt föreskrivas att personuppgiftsbiträdet ska

1. behandla personuppgifter bara enligt instruktioner från Försvarets radioanstalt,

2. säkerställa att personer som har tillstånd att behandla personuppgifter har förbundit sig att iaktta regler om tystnadsplikt eller omfattas av lagstadgad tystnadsplikt,

3. hjälpa Försvarets radioanstalt att säkerställa att bestämmelserna om de rättigheter som de som behandlingen rör har följts,

4. radera eller återlämna alla personuppgifter till Försvarets radioanstalt när uppdraget har slutförts och, om inte annat följer av lag eller förordning, radera befintliga kopior,

5. ge Försvarets radioanstalt tillgång till den information som krävs för att visa att det som sägs i denna bestämmelse, 9 § och 4 kap. 7, 9–11 §§ lagen (2019:000) om behandling av personuppgifter vid Försvarets radioanstalt följs, och

6. respektera de villkor som framgår av denna bestämmelse och 4 kap. 9 § lagen (2019:000) om behandling av personuppgifter vid Försvarets radioanstalt vid anlitande av ett annat personuppgiftsbiträde.

Övriga skyldigheter

9 § Det som sägs om Försvarets radioanstalts skyldigheter i 4 § gäller även för personuppgiftsbiträden som Försvarets radioanstalt anlitar.

5 kap. Enskildas rättigheter

Krav på utformningen av information

1 § Information enligt 5 kap. 1 och 2 §§ lagen (2019:000) om behandling av personuppgifter vid Försvarets radioanstalt ska vara lättillgänglig och lättbegriplig och lämnas i lämplig form.

Beslut

2 § Beslut enligt 5 kap. 2 och 5 §§ lagen (2019:000) om behandling av personuppgifter vid Försvarets radioanstalt ska vara skriftliga. Beslut som går den sökande emot ska motiveras.

Av 5 kap. 3 § andra stycket lagen (2019:000) om behandling av personuppgifter vid Försvarets radioanstalt framgår att skälen för vissa beslut inte behöver lämnas ut.

6 kap. Tillsyn

Tillsynsmyndighet

1 § Datainspektionen är tillsynsmyndighet enligt lagen (2019:000) om behandling av personuppgifter vid Försvarets radioanstalt.

Anmälningsskyldighet

2 § Om Datainspektionen i sin tillsyn uppmärksammar förhållanden som kan utgöra brott, ska myndigheten anmäla det till Åklagarmyndigheten.

Datainspektionen ska samråda med Åklagarmyndigheten innan en sådan anmälan görs. Till anmälan ska inspektionen foga det underlag som finns och även i övrigt lämna det bistånd som behövs i anledning av anmälan.

7 kap. Bemyndiganden

1 § Riksarkivet får, efter samråd med Försvarets radioanstalt, meddela föreskrifter om att personuppgifter som inte längre får behandlas enligt 2 kap. 19 § lagen (2019:000) om behandling av personuppgifter vid Försvarets radioanstalt ska bevaras. Sådana föreskrifter får dock inte omfatta personuppgifter som inte längre får behandlas enligt 3 kap. 1 § denna förordning.

2 § Försvarets radioanstalt får meddela närmare föreskrifter om verkställighet av bestämmelserna i lagen (2019:000) om behandling av personuppgifter vid Försvarets radioanstalt.

Om föreskrifterna berör integritetsskyddet vid personuppgiftsbehandling ska Försvarets radioanstalt samråda med Datainspektionen innan föreskrifterna beslutas.

---

1. Denna förordning träder i kraft den 1 oktober 2019.

2. Bestämmelserna i 3 kap. 10 § om loggning behöver inte tillämpas på uppgiftssamlingar som inrättats före ikraftträdandet förrän den 1 maj 2024.

1.8 Förslag till förordning om ändring i förordningen (2009:969) med instruktion för Statens inspektion för försvarsunderrättelseverksamheten

Härigenom föreskrivs att 1 och 3 §§ förordningen (2009:969) med instruktion för Statens inspektion för försvarsunderrättelseverksamheten ska ha följande lydelser.

Nuvarande lydelse	*Föreslagen lydelse*
1 §	
Statens inspektion för försvarsunderrättelseverksamheten har till uppgift att kontrollera försvarsunderrättelseverksamheten hos de myndigheter som enligt förordningen (2000:131) om försvarsunderrättelseverksamhet bedriver sådan verksamhet. Inspektionen ska kontrollera att dessa myndigheter, i den försvarsunderrättelseverksamhet som utförs, efterlever lagar och förordningar samt i övrigt fullgör sina skyldigheter.	
	Inspektionen har även till uppgift att lämna myndigheterna råd och stöd beträffande myndigheternas skyldigheter i den verksamhet som inspektionen har till uppgift att kontrollera och granska.
3 §	
Statens inspektion för försvarsunderrättelseverksamheten ska granska	
behandlingen av uppgifter enligt lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst samt enligt lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet.	*den behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst som sker med stöd av lagen (2019:000) om behandling av personuppgifter vid Försvarsmakten. Inspektionen ska även granska den behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och*

utvecklingsverksamhet som sker med stöd av lagen (2019:000) om behandling av personuppgifter vid Försvarets radioanstalt.

Denna förordning träder i kraft den 1 oktober 2019.

1.9 Förslag till förordning om ändring i förordningen (1995:1301) om handläggning av skadeståndsanspråk mot staten

Härigenom föreskrivs att 3 § förordningen (1995:1301) om handläggning av skadeståndsanspråk mot staten ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	3 §
	Justitiekanslern handlägger anspråk på ersättning med stöd av
	– 36 kap. 17 § andra stycket brottsbalken,
	– 2 kap. 1 § eller 3 kap. 1, 2 eller 4 § skadeståndslagen (1972:207), om anspråket grundas på ett påstående om felaktigt beslut eller underlåtenhet att meddela beslut,
	– 23 § datalagen (1973:289),
	– artikel 82 i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning),
2 kap. 6 § lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst och 2 kap. 5 § lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet,	*7 kap. 1 § lagen (2019:000) om behandling av personuppgifter vid Försvarsmakten* och *7 kap. 1 § lagen (2019:000) om behandling av personuppgifter vid Försvarets radioanstalt*,
	– lagen (1998:714) om ersättning vid frihetsberövanden och andra tvångsåtgärder, dock inte anspråk som avses i 8 § i den lagen,
	– 5 kap. 3 § lagen (2017:496) om internationellt polisiärt samarbete, om anspråket grundas på ett påstående om felaktigt beslut eller underlåtenhet att meddela beslut,
	– 26 § lagen (2011:111) om förstörande av vissa hälsofarliga missbrukssubstanser,
	– 46 kap. 20 § skatteförfarandelagen (2011:1244), eller
	– 44 § kameraövervakningslagen (2013:460).

Justitiekanslern handlägger också andra anspråk på ersättning som grundas på ett påstående om överträdelse av unionsrätten.

Av 4 § följer att vissa anspråk på ersättning med stöd av 3 kap. 1, 2 eller 4 § skadeståndslagen handläggs av Kammarkollegiet. Förordning (2018:303).

Denna förordning träder i kraft den 1 oktober 2019.

2 Utredningens uppdrag och arbete

2.1 Utredningsuppdraget

Utredningsuppdraget består i att göra en översyn av den lagstiftning som gäller för personuppgiftsbehandling inom Försvarsmakten och Försvarets radioanstalt och för att säkerställa att lagstiftningen är anpassad till den tekniska och legala utvecklingen.

Utredningen syftar till att analysera om rådande lagstiftning är ändamålsenlig för Försvarsmaktens och Försvarets radioanstalts verksamheter och om den är tillräcklig i fråga om skydd för enskildas personliga integritet Uppdraget omfattar även att utreda hur personuppgifter behandlas hos Försvarets radioanstalt i samband med att myndigheten stödjer andra myndigheter och statligt ägda bolag inom informationssäkerhetsområdet.

Om EU:s dataskyddsförordning, som trädde i kraft den 25 maj 2018, och därtill kopplad svensk författning skapar behov av kompletterande författningsbestämmelser för Försvarsmaktens och Försvarets radioanstalts personuppgiftsbehandling, ska utredningen även lämna förslag till sådana kompletterande bestämmelser.

Utredningens direktiv finns i bilaga 1.

Tilläggsdirektiv (förlängd tid för uppdraget) finns i bilaga 2.

2.2 Genomförande av uppdraget

Utredningsarbetet påbörjades i slutet av maj 2017 och har bedrivits på sedvanligt sätt med regelbundna utredningssammanträden med experter och sakkunniga. Utredningen har sammanträtt vid 17 tillfällen. Utredningen har besökt Försvarets radioanstalt, Försvarsmakten

och Statens inspektion för försvarsunderrättelseverksamheten (Siun) vid flera tillfällen.

Utredaren och sekreteraren har även samrått med Totalförsvarsdatautredningen (Fö 2016:01).

Föreningen Dataskydd.net har yttrat sig i en skrift som utredningen har tagit del av.

3 Försvarsmaktens och Försvarets radioanstalts uppgifter

3.1 Försvarsmaktens uppgifter

Försvarsmaktens grundläggande uppgifter framgår av 1–3 a §§ förordningen (2007:1266) med instruktion för Försvarsmakten (instruktionen för Försvarsmakten). Försvarsmakten har ett brett uppdrag som övergripande innebär ansvar för att upprätthålla och utveckla ett militärt försvar som ytterst kan möta ett väpnat angrepp. Grunden för Försvarsmaktens verksamhet ska vara förmågan till väpnad strid. Av bestämmelserna framgår vidare bl.a. att Försvarsmakten ska försvara Sverige och främja svensk säkerhet; upptäcka och avvisa kränkningar av det svenska territoriet; kunna delta i internationella militära insatser; genomföra räddnings-, evakuerings-, och förstärkningsinsatser; bedriva omvärldsbevakning och upptäcka och identifiera yttre hot mot Sverige och svenska intressen samt att ta fram underlag för beslut om höjd beredskap. Vid höjd beredskap ska Försvarsmakten kunna krigsorganisera, mobilisera och använda alla krigsförband för att möta ett militärt hot mot Sverige och svenska intressen. Krigsförband ska kunna krigsorganiseras även om höjd beredskap inte råder.

Försvarsmakten ska vidare, enligt 3 b § 1–4 instruktionen för Försvarsmakten särskilt bedriva verksamhet enligt lagen (2000:130) om försvarsunderrättelseverksamhet; leda och bedriva militär säkerhetstjänst; leda och samordna signalskyddstjänsten, inklusive arbetet med säkra kryptografiska funktioner som är avsedda att skydda skyddsvärd information, samt biträda Regeringskansliet i frågor som rör kryptoverksamhet och annan signalskyddsverksamhet. Försvarsmaktens underrättelseverksamhet beskrivs närmare i avsnitt 3.3.

Av instruktionen för Försvarsmakten följer även att Försvarsmakten, med myndighetens befintliga förmåga och resurser ska kunna lämna stöd till civil verksamhet; ansvara för att samla in, bearbeta

och lämna Kustbevakningen sjölägesinformation; på uppdrag av Försvarets materielverk bedriva exportrelaterad verksamhet inom försvarssektorn; medverka i statsceremonier och på begäran av polisen utföra helikoptertransporter som är av större vikt för genomförandet av polisiära insatser; bedriva militär luftfart; kunna bedriva internationell militär test-, utbildnings-, och övningsverksamhet i Sverige och genomföra utbildning för svenska och utländska deltagare avseende internationell fredsfrämjande, säkerhetsfrämjande och konfliktförebyggande verksamhet.

För att upprätthålla och utveckla ett militärt försvar krävs utveckling av teknik och metodik. Enligt 5 f § instruktionen för Försvarsmakten ska Försvarsmakten bl.a. bedriva egna studier och försök för inriktning och utveckling av det militära försvaret. Som ett exempel på när Försvarsmakten har behov av att bedriva dessa studier och försök kan nämnas regeringens uppdrag till Försvarsmakten att, med stöd av Försvarets radioanstalt, analysera och utveckla förmåga att genomföra aktiva operationer i cybermiljön för ett förstärkt cyberförsvar (Försvarsmaktens regleringsbrev för 2018).

Försvarsmakten ansvarar även jämte Säkerhetspolisen för den huvudsakliga tillsynen av säkerhetsskyddet i Sverige. Fördelningen myndigheterna emellan innebär att Säkerhetspolisen utövar tillsyn över myndigheter på det civila området och Försvarsmakten över myndigheter som hör till Försvarsdepartementet samt Försvarshögskolan och Fortifikationsverket (39 § säkerhetsskyddsförordningen [1996:633]). Sammantaget innebär regleringen i säkerhetsskyddsförordningen att Försvarsmakten och Säkerhetspolisen har rätt att utöva tillsyn i alla slag av verksamheter som säkerhetsskyddslagen (1996:627) gäller för, med undantag för Regeringskansliet, riksdagen och dess myndigheter och Justiekanslern. Till dessa verksamheter ska i stället Säkerhetspolisen på begäran lämna råd (47 § säkerhetsskyddsförordningen).

Här kan anmärkas att regeringen har föreslagit en ny säkerhetsskyddslag (prop. 2017/18:89). Den nya lagen föreslås träda i kraft den 1 april 2019.

Försvarsmakten har vidare vissa andra arbetsuppgifter som rör Sveriges försvar och säkerhet och som anges i lag eller förordning. Nedan ges ett antal exempel på sådana uppgifter.

1. Enligt förfogandelagen (1978:262) får Försvarsmakten under vissa omständigheter besluta att ta i anspråk egendom eller tjänster.
2. För att utreda och bedöma en totalförsvarspliktigs förutsättningar att fullgöra värnplikt kan Försvarsmakten genomföra annan utredning enligt 2 kap. 1 § lagen (1994:1809) om totalförsvarsplikt (3 kap. 5 § andra stycket förordningen [1995:238] om totalförsvarsplikt).
3. I lagen (2006:343) om Försvarsmaktens stöd till polisen vid terrorismbekämpning finns bestämmelser om Försvarsmaktens stöd till Polismyndigheten och Säkerhetspolisen vid terrorismbekämpning i form av insatser som kan innebära användning av våld eller tvång mot enskilda.
4. Försvarsmakten är enligt 4 § instruktionen för Försvarsmakten beslutsmyndighet enligt lagen (2006:939) om kvalificerade skyddsidentiteter i fall som avses i 2 § 3 den lagen.
5. Enligt förordningen (1982:314) om utnyttjande av Kustbevakningen inom Försvarsmakten ska personal ur Kustbevakningen inom Försvarsmakten användas för övervakning, transporter och andra uppgifter enligt närmare överenskommelse mellan myndigheterna.
6. Enligt förordningen (1992:391) om uttagning av egendom för totalförsvarets behov ska Försvarsmakten föra ett register över uttagen egendom och egendomens ägare.
7. Enligt förordningen om Sveriges försvarsattachéer (FFS 1985:20) ska en försvarsattaché, i det land eller de länder som han eller hon svarar för, följa och bedöma den militärpolitiska utvecklingen och utvecklingen i övrigt inom det totala försvaret, hålla sig underrättad om den säkerhetspolitiska utvecklingen samt i övrigt fullgöra uppgifter enligt Försvarsmaktens bestämmande.

Internationella samarbeten

Svensk säkerhet är beroende av internationella samarbeten och Sverige är en aktiv medlem i FN och EU. Sverige ingår också i ett partnerskap med Nato och bedriver bi- och multilaterala samarbeten på försvarsområdet med de nordiska och baltiska länderna, liksom med andra länder, t.ex. Storbritannien, Tyskland och USA.

Sverige utvecklar ett särskilt fördjupat försvarssamarbete med Finland. Som ett utslag av detta kan nämnas att det i SOU 2018:31 föreslås en lag om operativt militärt stöd mellan Sverige och Finland. Lagen syftar till att möjliggöra ett snabbare beslutsfattande om att, efter begäran från Finland, sätta in svenska väpnade styrkor för att stödja Finland med att hindra kränkningar av finskt territorium, samt att begära stöd från Finland i form av militära styrkor för att möta ett väpnat angrepp mot Sverige eller för att hindra kränkningar av svenskt territorium. Betänkandet bereds i Regeringskansliet.

Försvarsmakten deltar i de internationella samarbeten Sverige har på försvarsområdet, liksom i internationella fredsfrämjande och humanitära insatser. Försvarsmakten bidrar också till ett förstärkt underrättelsesamarbete inom ramen för EU:s gemensamma utrikes- och säkerhetspolitik och EU:s krishanteringsförmåga. Målsättningen för det internationella försvarssamarbetet är att effektivare använda resurser och öka den operativa förmågan för det svenska försvaret. Den svenska försvarsförmågan syftar ytterst till försvar av det egna territoriet men ska också betraktas som en del i en gemenskap för stabilitet och säkerhet i Europa.

3.2 Försvarets radioanstalts uppgifter

Försvarets radioanstalts uppgifter framgår av förordningen (2007:937) med instruktion för Försvarets radioanstalt. Av förordningen framgår bl.a. att Försvarets radioanstalt har till uppgift att bedriva signalspaning enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet och anslutande förordning (1 §).

Försvarets radioanstalt ska enligt 2 § förordningen med instruktion för Försvarets radioanstalt särskilt

1. följa förändringen av signalmiljön i omvärlden, den tekniska utvecklingen och signalskyddet,
2. fortlöpande utveckla den teknik och metodik som behövs för att bedriva verksamheten, och
3. utföra matematiska bedömningar av kryptosystem för totalförsvaret.

Enligt samma förordning ska Försvarets radioanstalt därutöver upprätthålla kompetensen för de nationella behoven i fråga om kryptologi (2 a §) samt biträda andra myndigheter vid värdering, utveckling, anskaffning och drift av signalspaningssystem (3 §).

Försvarets radioanstalt ska också stödja Försvarsmakten genom att utveckla metodik och utbilda personal inom signalspaningsområdet (3 a §), stödja Försvarsmaktens deltagande i internationella insatser med kompetens, personal och materiel (3 b §), vidmakthålla och utveckla signalreferensbibliotek för Försvarsmaktens behov (3 c §).

På uppdrag av Försvarets materielverk ska Försvarets radioanstalt utföra prov och utveckling inom teleteknikområdet (3 d §).

Försvarets radioanstalt ska ha hög teknisk kompetens inom informationssäkerhetsområdet och får efter begäran stödja sådana statliga myndigheter och statligt ägda bolag som hanterar information som bedöms vara känslig från sårbarhetssynpunkt eller i ett säkerhets- eller försvarspolitiskt avseende. Försvarets radioanstalt ska särskilt kunna stödja insatser vid nationella kriser med it-inslag, medverka till identifieringen av inblandade aktörer vid it-relaterade hot mot samhällsviktiga system, genomföra it-säkerhetsanalyser och ge annat tekniskt stöd. Försvarets radioanstalt ska samverka med andra organisationer inom informationssäkerhetsområdet såväl inom som utom landet (4 §).

Av Försvarets radioanstalts regleringsbrev för 2018 framgår att myndigheten ska fortsatt utveckla och på begäran kunna placera ut tekniska detekterings- och varningssystem (TDV) vid de mest skyddsvärda verksamheterna bland statliga myndigheter och statligt ägda bolag, som hanterar information som bedöms vara känslig från sårbarhetssynpunkt eller i ett säkerhets- eller försvarspolitiskt avseende.

Av regleringsbrevet för 2018 framgår vidare att myndigheten ska stödja Försvarsmakten i dess uppdrag att fortsätta analysera och utveckla förmåga att genomföra aktiva operationer i cybermiljön för ett förstärkt cyberförsvar.

3.3 Försvarsunderrättelseverksamhet

Försvarsunderrättelseverksamhet bedrivs enligt särskild reglering i bl.a. lagen (2000:130) och förordningen (2000:131) om försvarsunderrättelseverksamhet, samt i lagen (2008:717) och förordningen (2008:923) om signalspaning i försvarsunderrättelseverksamhet.

Av lagen om försvarsunderrättelseverksamhet framgår att försvarsunderrättelseverksamhet ska bedrivas till stöd för svensk utrikes-, säkerhets-, och försvarspolitik samt i övrigt för kartläggning av yttre hot mot landet samt att försvarsunderrättelseverksamhet endast får avse utländska förhållanden. I verksamheten ingår att medverka i svenskt deltagande i internationellt säkerhetssamarbete. Lagen anger vidare att regeringen ska bestämma försvarsunderrättelseverksamhetens inriktning. Inom ramen för denna inriktning får de myndigheter som regeringen bestämmer ange en närmare inriktning av verksamheten. Inriktning av signalspaning i försvarsunderrättelseverksamhet regleras i lagen om signalspaning i försvarsunderrättelseverksamhet, se avsnitt 3.3.5.

Avgränsningen till utländska förhållanden innebär att försvarsunderrättelseverksamheten typiskt sett ska inhämta, bearbeta, analysera och delge sådan information om företeelser och förhållanden i andra länder som ger svenska beslutsfattare ett förbättrat underlag för beslut och bedömningar i utrikes-, säkerhets- och försvarspolitiska frågor eller för att skydda svensk personal som deltar i internationella insatser. Verksamheten kan under vissa förhållanden även avse företeelser inom landet exempelvis om en organisation med verksamhet som utgör ett hot mot landet har sitt ursprung i ett annat land, men verkar genom representanter i Sverige eller genom att på annat sätt utnyttja resurser i Sverige. Det handlar då om att följa upp utländska förhållandens koppling till Sverige för att kunna bedöma hotbilden mot landet.

Enligt 2 § förordningen om försvarsunderrättelseverksamhet ska försvarsunderrättelseverksamhet bedrivas av Försvarsmakten, Försvarets radioanstalt, Försvarets materielverk och Totalförsvarets forskningsinstitut.

Försvarsunderrättelseverksamheten ska fullgöras genom inhämtning (teknisk och personbaserad), bearbetning och analys av information samt rapportering till berörda myndigheter (2 § lagen om försvarsunderrättelseverksamhet). Lagen hänvisar till att det i lagen

(2008:717) om signalspaning i försvarsunderrättelseverksamhet finns vissa bestämmelser om teknisk inhämtning.

De myndigheter som bedriver försvarsunderrättelseverksamhet får inte vidta åtgärder som syftar till att lösa uppgifter som enligt lagar eller andra föreskrifter ligger inom ramen för Polismyndighetens, Säkerhetspolisens och andra myndigheters brottsbekämpande och brottsförebyggande verksamheter. Om det inte finns hinder enligt andra bestämmelser, får de myndigheter som bedriver försvarsunderrättelseverksamhet emellertid lämna stöd till andra myndigheters brottsbekämpande och brottsförebyggande verksamhet (4 § lagen om försvarsunderrättelseverksamhet). Försvarsunderrättelseverksamhet som består i att genom tekniska metoder, såsom signalspaning, inhämta kommunikation anses inte utgöra en sådan åtgärd som avses i 4 §. Sådan verksamhet bedrivs nämligen inte på sådant sätt att den kan störa andra myndigheters verksamhet, och den syftar inte heller till att lösa en föreskriven uppgift för brottsbekämpande och brottsförebyggande verksamhet (jfr prop. 2006/07:63 s. 48).

Enligt 3 § lagen om försvarsunderrättelseverksamhet får de myndigheter som ska bedriva försvarsunderrättelseverksamhet, etablera och upprätthålla samarbete i underrättelsefrågor med andra länder och internationella organisationer. Enligt 3 § förordningen om försvarsunderrättelseverksamhet får samarbetet ske endast under förutsättning att syftet med samarbetet är att tjäna den svenska statsledningen och det svenska totalförsvaret. Det anges vidare att de uppgifter som myndigheterna lämnar till andra länder och internationella organisationer inte får vara till skada för svenska intressen. I den efterföljande paragrafen föreskrivs att myndigheterna ska anmäla frågor om att etablera och upprätthålla samarbetet och om viktiga frågor som uppkommer i samarbetet till Regeringskansliet (Försvarsdepartementet).

Exempel på vad som utgör försvarsunderrättelseverksamhet är säkerhetspolitiska och militärstrategiska bedömningar, analyser av pågående och framtida konflikter, internationella terroristgrupper, cyberhot, massförstörelsevapen samt biografiska underrättelser som avser utländsk militär personal eller andra viktiga befattningshavare.

Försvarsunderrättelseverksamheten går ut på att inom ramen för gällande inriktningar från uppdragsgivare upptäcka på förhand okända företeelser och uppgifter av relevans för dessa. Det kan exempelvis röra sig om uppgifter om nya hot mot svenska säkerhetsintressen, samhällsviktiga funktioner, eller mot svensk hemlig information

som inte får hamna hos främmande makt. Verksamheten innebär även att kartlägga redan kända företeelser och följa förändringar i dessa för att tidigt få kunskap om aktörers nya ambitioner, avsikter och förmågor.

Försvarsunderrättelseverksamhet är också ett centralt verktyg vid kartläggning i efterhand av händelser som oförutsett inträffat, i syfte att finna förklaringar till det inträffade samt för att kartlägga eventuella ännu inte identifierade inslag i en inträffad händelse. Genom sådan uppföljning kan ytterligare underrättelseinformation produceras som ger dels bättre förståelse för orsakerna bakom det inträffade, dels kompletterande information om inslag som ännu inte identifierats, t.ex. kvarvarande oupptäckta hot.

3.3.1 Försvarsmaktens underrättelseverksamhet och militära säkerhetstjänst

Den underrättelseverksamhet som bedrivs inom Försvarsmakten kan i rättsligt hänseende i huvudsak hänföras till försvarsunderrättelseverksamhet, militär säkerhetsunderrättelsetjänst och övrig militär underrättelseverksamhet. Den militära säkerhetstjänsten inbegriper, förutom säkerhetsunderrättelsetjänst, säkerhetsskydd och signalskydd.

3.3.2 Försvarsmaktens försvarsunderrättelseverksamhet

Av Försvarsmaktens arbetsordning framgår att det är chefen för den militära underrättelse- och säkerhetstjänsten (Must) som ska planera, leda, genomföra och följa upp försvarsunderrättelseverksamheten inom Försvarsmakten (11 kap. 1 § Försvarsmaktens föreskrifter med arbetsordning för Försvarsmakten, FFS 2016:2).

Av lagstiftningen följer att försvarsunderrättelseverksamhet ska följa regeringens inriktning och Försvarsmaktens samt ett antal andra myndigheters närmare inriktning. Dessa inriktningar är hemliga.

Rapportering sker kontinuerligt i form av föredragningar, dialoger och skriftliga rapporter.

För att lösa sina uppgifter har Must ett antal egna källor och möjligheten att ha samarbeten med utländska myndigheter och internationella organisationer. Must får även information från bland andra

Säkerhetspolisen och Försvarets radioanstalt inom ramen för gällande regelverk.

3.3.3 Försvarsmaktens militära säkerhetstjänst

Av 3 b § instruktionen för Försvarsmakten framgår att Försvarsmakten särskilt ska leda och bedriva militär säkerhetstjänst. I säkerhetsskyddslagen (1996:627) finns bestämmelser om säkerhetsskydd. Med säkerhetsskydd avses enligt 6 § säkerhetsskyddslagen 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 offentlighets- och sekretesslagen (2009:400) och som rör rikets säkerhet. Vidare avses med säkerhetsskydd även skydd mot terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott, även om brotten inte hotar rikets säkerhet.

Den militära säkerhetstjänstens uppgift är att skydda de säkerhetsintressen som berör Försvarsmakten och dess tillsynsområde enligt säkerhetsskyddslagstiftningen. Den militära säkerhetstjänsten ska samverka med Säkerhetspolisen och Polismyndigheten. Den militära säkerhetstjänsten ska också samverka med Myndigheten för samhällsskydd och beredskap och andra myndigheter rörande säkerhetsintressen som berör totalförsvaret.

Säkerhetsintressena omfattar, eller kan hänföras till personal, materiel, information, anläggningar och verksamhet. Med begreppet militär säkerhetstjänst avses såväl verksamheten som dess organisation. Den militära säkerhetstjänsten består av säkerhetsunderrättelsetjänst, säkerhetsskyddstjänst och signalskyddstjänst. Den kan riktas mot hela eller delar av Försvarsmakten, viss funktion eller verksamhet och förband samt verksamhet inom Försvarsmaktens intresseområde, t.ex. försvarsindustri (se prop. 2006/07:46 s. 25).

Säkerhetsunderrättelsetjänsten har till uppgift att klarlägga och analysera den säkerhetshotande verksamhetens mål, medel och metoder. Säkerhetshotande verksamhet mot Sverige eller mot insatta förband och insatser i andra länder kan förekomma i form av främmande underrättelseverksamhet, sabotage, subversiv verksamhet, terrorism och kriminalitet. Säkerhetsunderrättelsetjänst bedrivs genom planläggning, inhämtning, bearbetning och analys samt delgivning av säkerhetsunderrättelser.

Säkerhetsskyddstjänstens uppgift är att ta fram åtgärder som syftar till att hindra eller försvåra säkerhetshotande verksamhet såsom exempelvis obehörigt röjande av hemliga uppgifter som rör Sveriges säkerhet, sabotage, stöld och terrorism. Säkerhetsskyddstjänsten ska, utifrån hotbild och säkerhetshotande verksamhet, ge säkerhetsintressena relevant skydd i form av informationssäkerhet, tillträdesbegränsning och säkerhetsprövning.

Signalskyddstjänsten syftar till att förhindra obehörig insyn i och påverkan av telekommunikations- och it-system med hjälp av kryptografiska metoder och övriga signalskyddsåtgärder. Signalskyddstjänsten är en säkerhetsskyddsangelägenhet där ansvaret omfattar hela totalförsvaret och syftet är att säkerställa säker kommunikation.

En del av signalskyddstjänsten är kontroll av signalskyddet i telekommunikations- och it-system, s.k. signalkontroll. Signalkontroll syftar till att klarlägga riskerna för obehörig åtkomst till eller förvanskning av uppgifter eller störning av telekommunikation. Vidare kan signalkontroll klarlägga att systemen används enligt gällande regelverk (prop. 2006/07:46 s. 25 f.).

Säkerhetsskyddstjänsten och signalskyddstjänsten syftar gemensamt till att förebygga, förhindra och motverka säkerhetshotande verksamhet. Tillsyn, utbildning, uppföljning och kontroll är nödvändiga beståndsdelar för att uppnå ett fullgott säkerhetsskydd.

Chefen för militära underrättelse- och säkerhetstjänsten ansvarar för Försvarsmaktens tillsyn vad avser säkerhetsskyddet vid Fortifikationsverket, Försvarshögskolan och de myndigheter som hör till Försvarsdepartementet (11 kap. 12 § första stycket 6 Försvarsmaktens föreskrifter med arbetsordning för Försvarsmakten, FFS 2016:2).

3.3.4 Övrig militär underrättelseverksamhet

Övrig militär underrättelseverksamhet utgörs av den underrättelsetjänst som Försvarsmakten genomför för att kunna lösa Försvarsmaktens militära uppgifter såsom dessa uppgifter framträder exempelvis i Försvarsmaktens instruktion, regleringsbrev eller särskilda regeringsbeslut och som inte utgör försvarsunderrättelseverksamhet eller militär säkerhetstjänst. Denna underrättelseverksamhet syftar främst till i att skapa en lägesbild och ge beslutsunderlag för militära chefer.

Must bedriver t.ex. militär underrättelsetjänst till stöd för Överbefälhavaren (ÖB), i enlighet med dennes inriktning. Uppgifterna till Must omfattar stöd med bedömningar för ÖB:s långsiktiga utveckling av Försvarsmaktens förmågor och förband, försvarsplanläggning, ledning, planering och genomförande av militära insatser i närområdet och i de internationella insatsområdena. Must är ålagd att kontinuerligt följa den militära utvecklingen och verksamheten i närområdet.

3.3.5 Försvarets radioanstalts signalspaning i försvarsunderrättelse- och utvecklingsverksamhet

Signalspaning, inhämtning av signaler i elektronisk form, är en inhämtningsmetod i försvarsunderrättelseverksamheten som regleras i lagen om signalspaning i försvarsunderrättelseverksamhet. Inriktning av signalspaning får endast anges av regeringen, Regeringskansliet, Försvarsmakten, Säkerhetspolisen och Nationella operativa avdelningen vid Polismyndigheten (4 §).

Av 1 § lagen om signalspaning i försvarsunderrättelseverksamhet följer att signalspaning endast får avse utländska förhållanden och ske i syfte att kartlägga vissa i lagen särskilt uppräknade företeelser:

1. yttre militära hot mot landet,
2. förutsättningar för svenskt deltagande i fredsfrämjande och humanitära internationella insatser eller hot mot säkerheten för svenska intressen vid genomförandet av sådana insatser,
3. strategiska förhållanden avseende internationell terrorism och annan grov gränsöverskridande brottslighet som kan hota väsentliga nationella intressen,
4. utveckling och spridning av massförstörelsevapen, krigsmateriel och produkter som avses i lagen (2000:1064) om kontroll av produkter med dubbla användningsområden och av tekniskt bistånd,
5. allvarliga yttre hot mot samhällets infrastrukturer,
6. konflikter utomlands med konsekvenser för internationell säkerhet,
7. främmande underrättelseverksamhet mot svenska intressen, eller

8. främmande makts agerande eller avsikter av väsentlig betydelse för svensk utrikes-, säkerhets- eller försvarspolitik.

Försvarets radioanstalt ska ansöka om tillstånd hos Försvarsunderrättelsedomstolen för den signalspaning som får utföras enligt lagen (4 a §), varefter domstolen meddelar tillstånd om vissa krav är uppfyllda, bl.a. att syftet med inhämtningen inte kan tillgodoses på ett mindre ingripande sätt och uppdraget beräknas ge information vars värde är klart större än det integritetsintrång som inhämtning i enlighet med ansökan kan innebära (5 §).

Signalspaning i försvarsunderrättelseverksamhet syftar alltid till att rapportera underrättelser som ger ett kompletterande mervärde för uppdragsgivarna utöver den rapportering och det öppna informationsflöde som de i övrigt kan ta del av. Det sker genom att Försvarets radioanstalt inhämtar information som är relevant för att tillgodose de underrättelsebehov som regeringen och andra uppdragsgivare uttryckt i en inriktning.

Det är normalt sett informationen, inte den källa som för stunden hanterar eller förmedlar information, som är det centrala. Inom vissa underrättelseområden, t.ex. främmande underrättelseverksamhet och terrorism, kan dock enskilda källor vara centrala om de i sig kan utgöra ett hot mot Sverige och svenska intressen.

Signalspaningen är en viktig del av Sveriges försvarsunderrättelseverksamhet och bidrar till att ge regeringen underlag för en självständig svensk utrikes-, säkerhets- och försvarspolitik och till att ge andra inriktande myndigheter kvalificerad underrättelseinformation om utländska förhållanden för att de i sin tur ska kunna fullgöra sina uppgifter.

All signalspaning vid Försvarets radioanstalt sker inom ramen för givna inriktningar. De enskilda, i varje givet ögonblick, mest angelägna konkreta underrättelsefrågorna kan ofta inte ställas i förväg då de ännu inte är kända. Omvärlden förändras fortlöpande och därmed de konkreta underrättelsebehoven. Av detta följer att Försvarets radioanstalt behöver vara väl förberedd på nya frågeställningar genom att ständigt utveckla förmågor att hitta och identifiera nya relevanta källor till information.

Den information som Försvarets radioanstalt strävar efter att finna och rapportera, i syfte att tillgodose uttryckta underrättelsebehov, är ofta konfidentiell och således skyddsvärd för den källa som

hanterar informationen. Informationen är därför ofta försedd med någon form av åtkomstskydd för att förhindra obehörig åtkomst. För att framgångsrikt bedriva försvarsunderrättelse- och utvecklingsverksamhet krävs därför aktuell och ingående kunskap dels om hur signaler förmedlas och hanteras i elektronisk form, dels om de mekanismer som används för att skydda informationen.

För att kunna tillgodose uppdragsgivarnas underrättelsebehov behöver Försvarets radioanstalt ingående kunskap om signalmiljön för att på ett effektivt sätt kunna rikta inhämtningskapacitet mot rätt delar av signalmiljön samt för att kunna urskilja, extrahera och tyda den relevanta informationen. För detta krävs omfattande expertkunskaper om såväl signalmiljöns struktur som dess användning. Försvarets radioanstalt bedriver därför en utvecklingsverksamhet för att etablera och upprätthålla en tillräckligt god förståelse av signalmiljön, samt tillräckligt god förmåga att kunna bedriva inhämtning, bearbetning och analys av den information som förekommer i signalmiljön. Om det är nödvändigt för försvarsunderrättelseverksamheten får enligt 1 § tredje stycket lagen om signalspaning i försvarsunderrättelseverksamhet signaler i elektronisk form även inhämtas vid signalspaning för att följa förändringar i signalmiljön i omvärlden, den tekniska utvecklingen och signalskyddet samt för att fortlöpande utveckla den teknik och metodik som behövs för att bedriva verksamheten.

Utvecklingsverksamheten har således inte något självständigt existensberättigande, utan syftar enbart till att etablera och vidmakthålla fortsatt förmåga som är nödvändig för försvarsunderrättelseverksamheten.

3.3.6 Försvarets radioanstalts informationssäkerhetsverksamhet

Som beskrivits i avsnitt 3.2 har Försvarets radioanstalt ett särskilt uppdrag att lämna stöd så att informationssäkerheten kan upprätthållas vid de mest skyddsvärda verksamheterna i Sverige. Försvarets radioanstalt har även till uppgift enligt 17 § förordningen (2015:1053) om totalförsvar och höjd beredskap att tilldela säkra kryptografiska funktioner till ett antal civila myndigheter och organisationer.

Försvarets radioanstalt möjlighet att hantera de allvarligaste it-angreppen mot de mest skyddsvärda verksamheterna kräver en förmåga att upptäcka dessa samt att kartlägga bakomliggande aktörer. Signalspaning har en avgörande betydelse för att Försvarets radioanstalt ska kunna förse uppdragsgivare med unika underrättelser kring it-relaterade hot mot Sverige och svenska intressen. Samma underrättelser kan inom Försvarets radioanstalts informationssäkerhetsverksamhet omsättas till indirekt och direkt skydd som omfattar såväl tekniska tjänster (exempelvis signalskydd, sensorsystem och informationssäkerhetsanalyser) som rådgivning och utbildning.

Ett tydligt exempel på detta ömsesidiga utbyte av information är det tekniska detekterings- och varningssystem (TDV) som Försvarets radioanstalt tagit fram på uppdrag av regeringen. TDV erbjuds de mest skyddsvärda verksamheter som redan har uppnått en egen god informationssäkerhet, ofta med stöd av Försvarets radioanstalt. Genom signaturer från signalspaning upptäcker systemet avancerade angrepp som kommersiella antivirusprogram inte kan hitta. Samtidigt kan det återkommande stöd som Försvarets radioanstalt ger de mest skyddsvärda verksamheterna, ge signalspaningen ny kunskap om tidigare okända angreppsmetoder, tillvägagångssätt eller aktörer. Genom att tillvarata synergierna mellan försvarsunderrättelse- och informationssäkerhetsverksamheten skapas således viktiga mervärden.

4 Gällande rätt

4.1 Internationella överenskommelser

4.1.1 Förenta nationerna

Förenta nationernas (FN) allmänna förklaring om de mänskliga rättigheterna antogs år 1948 av FN:s generalförsamling. Förklaringen omfattar politiska, medborgerliga, sociala, ekonomiska och kulturella rättigheter. Även om den allmänna förklaringen inte är bindande för medlemsstaterna ses den som ett uttryck för den internationella opinionens krav. Skyddet för den personliga integriteten behandlas i artikel 12. Där anges att ingen får utsättas för godtyckligt ingripande i fråga om privatliv, familj, hem eller korrespondens och inte heller för angrepp på sin heder eller sitt anseende. Var och en har rätt till lagens skydd mot sådana ingripanden och angrepp. Vidare anges i artikel 29 att en person endast får underkastas sådana inskränkningar som har fastställts i lag och enbart i syfte att trygga tillbörlig hänsyn till och respekt för andras fri- och rättigheter samt för att tillgodose ett demokratiskt samhälles berättigade krav på moral, allmän ordning och allmän välfärd. FN har också antagit den internationella konventionen om medborgerliga och politiska rättigheter som trädde i kraft år 1976, till vilken Sverige är ansluten. Skyddet för den personliga integriteten regleras i artikel 17 i konventionen, vilken till sitt innehåll är likvärdig med ovan nämnda artikel 12 i den allmänna förklaringen. Kommittén för de mänskliga rättigheterna har inrättats för att övervaka att medlemsstaterna efterlever sina skyldigheter enligt konventionen. I sammanhanget bör också nämnas att FN:s generalförsamling år 1990 antog riktlinjer om datoriserade register med personuppgifter. Enligt riktlinjerna får medlemsstaterna i den nationella lagstiftningen avseende datoriserade register med personuppgifter inte samla in eller behandla personuppgifter på ett olagligt sätt eller använda uppgifterna för syften som står i strid med FN:s

stadga. Ändamålet med ett register ska vara specificerat, berättigat och på något sätt uttryckligt angivet för den som berörs. Detta för att försäkra att alla personuppgifter som samlas in och behandlas är relevanta och adekvata för det angivna ändamålet, att uppgifterna inte används i strid med ändamålet och att uppgifterna inte bevaras längre än som krävs för att uppfylla det angivna ändamålet.

4.1.2 OECD

Organisationen för ekonomiskt samarbete och utveckling (OECD) har utarbetat riktlinjer angående integritetsskyddet och flödet av personuppgifter över gränserna. Riktlinjerna antogs år 1980 av OECD:s råd samtidigt som en rekommendation till medlemsländernas regeringar om att beakta riktlinjerna i nationell lagstiftning. Sverige har godtagit rekommendationerna och därmed åtagit sig att följa riktlinjerna. Riktlinjerna, som är att betrakta som minimiregler, motsvarar i princip bestämmelserna i Europarådets dataskyddskonvention och är tillämpliga på personuppgifter inom både den offentliga och den privata sektorn. Riktlinjerna gäller såväl för uppgifter som lagras automatiskt som uppgifter som förs manuellt. Riktlinjerna innehåller grundläggande principer till skydd för den personliga integriteten, bl.a. att personuppgifter ska vara relevanta för de ändamål för vilka de ska användas. Vidare anges att personuppgifterna även ska vara riktiga och fullständiga samt hållas aktuella. En annan grundläggande princip är att de ändamål för vilka personuppgifterna samlades in ska vara preciserade senast vid insamlingen.

4.2 Europarätt

4.2.1 Europarådet

Europakonventionen

De rättigheter som anges i FN:s allmänna förklaring om de mänskliga rättigheterna har utvecklats vidare i Europakonventionen.

Europakonventionen gäller sedan den 1 januari 1995 som lag i Sverige (lagen [1994:1219] om den europeiska konventionen angående skydd för de mänskliga rättigheterna och grundläggande friheterna). Av 2 kap. 19 § regeringsformen framgår att lag eller annan föreskrift

inte får meddelas i strid med Sveriges åtaganden på grund av konventionen. Det är framför allt artikel 8 i konventionen som har betydelse för skyddet av den personliga integriteten. Av artikeln framgår 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 rätt annat än med stöd av lag och om det i ett demokratiskt samhälle är nödvändigt med hänsyn till statens säkerhet, den allmänna säkerheten, landets ekonomiska välstånd, till förebyggande av oordning eller brott, till skydd för hälsa och moral eller för andra personers fri- och rättigheter. Tillämpningsområdet för artikeln omfattar behandling av personuppgifter om privatliv, familjeliv, hem eller korrespondens. Artikeln innebär att staten ska avhålla sig från ingrepp i den skyddade rättigheten men också en skyldighet för staten att vidta åtgärder för att skydda den enskildes privata sfär (Danelius, H., Mänskliga rättigheter i europeisk praxis, 4 uppl., 2012, s. 347 f.). En inskränkning i en konventionsskyddad rättighet ska ha stöd i lag. Lagen ska vara så preciserad att inskränkningarna är förutsebara och att lagen är allmänt tillgänglig. Europadomstolen har i praxis slagit fast att intrånget ska vara nödvändigt, dvs. det ska finnas ett ”angeläget samhälleligt behov” och inskränkningen ska stå i rimlig proportion till det syfte som ska tillgodoses genom den.

Europarådets dataskyddskonvention

De dataskyddsregler som antagits inom ramen för Europarådet finns i första hand i Europarådets konvention om skydd för enskilda vid automatisk databehandling av personuppgifter[1] (ETS 108), den s.k. dataskyddskonventionen. Konventionen, som trädde i kraft den 1 oktober 1985, kompletteras av ett antal av ministerkommittén antagna icke bindande rekommendationer om hur personuppgifter bör behandlas inom olika områden. Dataskyddskonventionen gäller för Europarådets 47 medlemsstater, men även Mauritius, Senegal, Tunisien och Uruguay är parter till konventionen.

Konventionen brukar ses som en precisering av artikel 8 i Europakonventionen och syftar till att säkerställa respekten för grundläggande fri- och rättigheter, särskilt den enskildes rätt till personlig

[1] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108).

integritet i samband med automatiserad behandling av personuppgifter (artikel 1). Konventionen tar sikte på behandling av personuppgifter i automatiserade personregister och automatiserad personuppgiftsbehandling i allmän och enskild verksamhet. Personuppgifterna ska enligt konventionen inhämtas och behandlas på ett korrekt sätt och de ska vara relevanta med hänsyn till ändamålet (artikel 5). Vissa kategorier av personuppgifter får inte behandlas genom automatiserad databehandling om inte den nationella lagstiftningen ger ett ändamålsenligt skydd (”appropriate safeguards”). Till sådana kategorier hör personuppgifter som avslöjar ras, politisk tillhörighet, religiös tro eller övertygelse i övrigt, sexualliv samt uppgifter om brott (artikel 6).

Konventionen innehåller även enskildas rätt att veta att information lagras om honom eller henne och rätten att vid behov få den korrigerad (artikel 8). Restriktioner när det gäller rättigheterna i konventionen är endast möjliga när det handlar om ett överordnat intresse, såsom statens säkerhet eller försvar (artikel 9).

Enligt artikel 10 i dataskyddskonventionen, som även omfattar personuppgiftsbehandling som rör nationell säkerhet, åtar sig konventionsstaterna att införa lämpliga sanktioner och rättsmedel (”appropriate sanctions and remedies”) för överträdelser av sådana bestämmelser i den nationella lag genom vilka de grundläggande principer för dataskydd som har angetts i konventionen har genomförts. Konventionen anger dock inte vilka krav som ställs på sådana sanktioner.

Europarådets ministerkommitté antog år 2001 ett tilläggsprotokoll till dataskyddskonventionen (ETS 181). Det innehåller bestämmelser om tillsynsmyndigheter och överföring av personuppgifter till länder som inte är bundna av konventionen. Tilläggsprotokollet trädde i kraft den 1 juli 2004. Av protokollet framgår bl.a. att varje konventionsstat ska se till att en eller flera myndigheter ansvarar för att kontrollera att de åtgärder respekteras som inom dess nationella lagstiftning ger verkan åt de principer som anges i konventionen. Tilläggsprotokollet innehåller vidare bestämmelser som anger att konventionsstaterna ska vidta åtgärder för att säkerställa att överföring av personuppgifter till ett land som inte är konventionspart får ske bara om landet i fråga säkerställer en adekvat skyddsnivå för uppgifterna.

Konventionens roll som grundläggande dokument för automatiserad behandling av personuppgifter inom EU har i princip över-

tagits av EU:s reglering i form av direktiv och förordning. EU:s reglering omfattar emellertid inte behandling av personuppgifter inom områden som allmän säkerhet, försvar och statens säkerhet (dvs. utanför unionsrätten). På dessa områden är dataskyddskonventionen därför fortfarande av betydelse.

Europarådet inledde år 2010 en översyn av konventionen och rekommendationerna. Europarådets medlemsstater antog ett ändringsprotokoll den 18 maj 2018. Ändringsprotokollet träder i kraft när det har ratificerats av Europarådets alla 47 medlemsstater. Ändringsprotokollet kan också träda i kraft om det har ratificerats av 38 medlemsstater, men gäller följaktligen då endast för de stater som har ratificerat protokollet.[2]

4.2.2 Europeiska unionen

Stadgan

Av Europeiska unionens stadga om de grundläggande rättigheterna[3] framgår att var och en har rätt till skydd av de personuppgifter som rör honom eller henne. Sådana uppgifter ska behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund. Var och en har rätt att få tillgång till insamlade uppgifter som rör honom eller henne och att få rättelse av dem. En oberoende myndighet ska kontrollera att dessa regler efterlevs (artikel 8).

I artikel 52 i stadgan anges i vilken utsträckning inskränkningar får göras i de rättigheter som erkänns i stadgan. Utgångspunkten är att sådana inskränkningar endast får göras i lag och ska vara förenliga med det väsentliga innehållet i rättigheterna. Begränsningar får endast göras om de är nödvändiga och svarar mot ett allmänt samhällsintresse som erkänns av unionen eller behovet av skydd för andra människors rättigheter och friheter.

[2] Ändringsprotokollet (Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), som antogs på Europarådets ministermöte i Helsingör, Danmark, finns tillgängligt på Europarådets hemsida: www.coe.int

[3] Europeiska unionens stadga om de grundläggande fri- och rättigheterna (2010/C 83/02).

EU-stadgan är rättsligt bindande för medlemsstaterna vid tillämpning av unionsrätten. Stadgan ska således inte tillämpas på nationell lagstiftning inom områden där EU inte har lagstiftningskompetens.[4]

1995 års dataskyddsdirektiv

Den allmänna regleringen av personuppgiftsbehandling inom Europeiska unionen fanns till den 25 maj 2018 i 1995 års dataskyddsdirektiv. Direktivet syftade till att garantera en hög och i alla medlemsstater likvärdig skyddsnivå när det gäller enskilda personers fri- och rättigheter med avseende på behandling av personuppgifter och att främja ett fritt flöde av personuppgifter mellan medlemsstaterna i EU. Direktivet, som har genomförts i svensk rätt huvudsakligen genom personuppgiftslagen (1998:204) med tillhörande förordning gällde inte för behandling av personuppgifter utanför unionsrätten, t.ex. allmän säkerhet, försvar, statens säkerhet och statens verksamhet på straffrättens område. Personuppgiftslagen redogörs närmare för i avsnitt 4.3.3.

EU:s dataskyddsreform

Europeiska kommissionen presenterade i januari 2012 förslag till en genomgripande reform av EU:s regler om skydd för personuppgifter. Reformen omfattar dels en allmän dataskyddsförordning som ersätter 1995 års dataskyddsdirektiv, dels ett nytt direktiv (2016 års dataskyddsdirektiv) med särregler för personuppgiftsbehandling i främst den brottsbekämpande sektorn.

EU:s dataskyddsförordning och 2016 års dataskyddsdirektiv är tvingande endast inom unionsrätten och innehåller också uttryckliga undantag för behandling av personuppgifter som sker inom verksamhet som inte omfattas av unionsrätten.

[4] Lissabonfördraget artikel 6.

EU:s dataskyddsförordning

Allmänt

Sedan den 25 maj 2018 utgör Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), hädanefter *EU:s dataskyddsförordning* eller *dataskyddsförordningen*, grunden för generell personuppgiftsbehandling inom EU. Det huvudsakliga syftet med dataskyddsförordningen är bl.a. att säkerställa en enhetlig skyddsnivå över hela unionen och att undvika avvikelser som hindrar den fria rörligheten av personuppgifter inom den inre marknaden. Dataskyddsförordningen är direkt tillämplig i alla EU:s medlemsstater men förutsätter och möjliggör samtidigt kompletterande och specificerande nationella bestämmelser av olika slag.

Behandling av personuppgifter som sker inom verksamhet som inte omfattas av EU-rätten, t.ex. försvar och nationell säkerhet, behandling som sker inom EU:s gemensamma utrikes- och säkerhetspolitik, behandling som utförs av en fysisk person och som är av rent privat natur samt behandling som sker inom brottsbekämpande verksamhet, är uttryckligen undantagna från tillämpningsområdet (artikel 2).

Dataskyddsförordningen reglerar bl.a. grundläggande principer för behandling av personuppgifter, den registrerades rättigheter, personuppgiftsansvar, tillsyn över personuppgiftsbehandling och rätten för enskilda att få tillgång till rättsmedel och sanktioner mot ansvariga som inte lever upp till förordningens krav. I förhållande till tidigare lagstiftning ställer dataskyddsförordningen högre krav på de personuppgiftsansvariga genom bestämmelser om bl.a. utökad informationsskyldighet och möjlighet att besluta om administrativa sanktionsavgifter (artikel 83). Dessutom inrättas Europeiska dataskyddsstyrelsen med representanter från samtliga EU-länders dataskyddsmyndigheter, däribland Datainspektionen (artikel 68). Styrelsen har befogenhet att fatta beslut i frågor där nationella tillsynsmyndigheter inte kan komma överens, ge råd och vägledning om hur dataskyddsförordningen ska tillämpas och godkänna EU-omfattande uppförandekoder och certifieringar.

I Sverige

Utöver dataskyddsförordningen gäller sedan den 25 maj 2018 även lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen). Samtidigt som denna lag trädde i kraft upphävdes personuppgiftslagen.

Enligt 1 kap. 2 § dataskyddslagen gäller bestämmelserna i EU:s dataskyddsförordning och dataskyddslagen även vid behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av unionsrätten. Europeiska dataskyddsstyrelsen saknar emellertid behörighet inom detta utvidgade tillämpningsområde (se prop. 2017/18:105 s. 184).

Särskilda undantag från detta utvidgade tillämpningsområde har gjorts för bl.a. lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst och lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet.

Enligt övergångsbestämmelserna i dataskyddslagen ska personuppgiftslagen fortsätta att gälla i sådan verksamhet hos Försvarsmakten, Försvarets radioanstalt och Totalförsvarets rekryteringsmyndighet som *inte* omfattas av unionsrätten. Övergångsbestämmelserna gäller av förklarliga skäl inte sådan personuppgiftsbehandling som omfattas av Försvarsmaktens och Försvarets radioanstalts ovan nämnda särlagstiftning.

2016 års dataskyddsdirektiv

Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016[5] (2016 års dataskyddsdirektiv) innehåller särregler för den personuppgiftsbehandling som behöriga myndigheter utför bl.a. i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott samt för att skydda mot, förebygga och förhindra hot mot den allmänna

[5] Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF.

säkerheten. Direktivet ersätter det gällande dataskyddsrambeslutet (2008/977/RIF)[6] som reglerar utbyte av personuppgifter mellan medlemsstaterna inom denna sektor. Direktivets tillämpningsområde omfattar, till skillnad från rambeslutet, även rent nationell personuppgiftsbehandling på området för brottsbekämpning, brottmålshantering och straffverkställighet.

EU:s nya dataskyddsdirektiv har i huvudsak genomförts genom en ny ramlag, brottsdatalagen (2018:1177) som träder i kraft den 1 augusti 2018. Syftet med lagen är både att skydda fysiska personers grundläggande fri- och rättigheter och att säkerställa att behöriga myndigheter kan behandla och utbyta personuppgifter med varandra på ett ändamålsenligt sätt. Lagen är, liksom tidigare personuppgiftslagen, subsidiär i förhållande till annan lag eller förordning, vilket möjliggör avvikande bestämmelser i s.k. registerförfattningar.

Brottsdatalagen reglerar inte Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet eller om Polismyndigheten har övertagit en arbetsuppgift som rör nationell säkerhet från Säkerhetspolisen. Utredningen om 2016 års dataskyddsdirektiv har föreslagit att dessa områden ska regleras särskilt (SOU 2017:74). Förslaget bereds i Regeringskansliet.

Brottsdatalagen kan även bli tillämplig i vissa delar av Försvarsmaktens verksamhet, t.ex. när militärpolisen och militära skyddsvakter utför uppgifter med polismans befogenhet. Motsvarande kan gälla i samband med att Försvarsmakten lämnar stöd till polisen vid terrorismbekämpning. Nu nämnda exempel kan dock också komma att utföras inom ramen för Försvarsmaktens militära säkerhetstjänst. Av 4 § brottsdatalagen framgår därför att lagen inte är tillämplig i sådan verksamhet som omfattas av lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst (se prop. 2017/18:232 s. 14 och 102 f.).

[6] Rådets rambeslut 2008/977/RIF av den 27 november 2008 om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete. Genomfört i svensk rätt huvudsakligen genom personuppgiftslagen (1998:204) med kompletterande bestämmelser i lag (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen (2013 års lag).

4.3 Nationell reglering till skydd för den personliga integriteten

4.3.1 Rätten till personlig integritet

Svensk rätt saknar en allmängiltig definition av begreppet personlig integritet. Någon entydig definition finns inte heller i internationell rätt[7].

Ett sätt att bestämma begreppet personlig integritet är att ange vilka handlingar som utgör kränkningar av densamma. Enligt denna modell, som använts i bl.a. prop. 2006/07:63, En anpassad försvarsunderrättelseverksamhet (s. 61), kan kränkningarna delas in i tre huvudgrupper: 1) intrång i en persons privata sfär i fysisk eller annan mening, 2) insamlande av uppgifter om en persons privata förhållanden och 3) offentliggörande eller annan användning (t.ex. som bevisning i rättegång) av uppgifter om en persons privata förhållanden. Som konkreta exempel på olika slag av kränkningar angavs intrång i en persons privata sfär genom bl.a. olovlig ljudupptagning, brytande av brevhemlighet, telefonavlyssning och utnyttjande av elektronisk avlyssningsapparatur.

Den personliga integriteten kan alltså kränkas på många olika sätt. Även om det inte finns någon entydig definition av begreppet kan konstateras att kränkningarna innebär ett intrång i en fredad sfär som den enskilde bör vara tillförsäkrad.

4.3.2 Regeringsformen

Regeringsformen innehåller grundläggande bestämmelser till skydd för den personliga integriteten. Enligt målsättningsstadgandet i 1 kap. 2 § första stycket ska den offentliga makten utövas med respekt bl.a. för den enskilda människans frihet och enligt fjärde stycket ska det allmänna värna om den enskildes privat- och familjeliv. Bestämmelserna har dock inte någon bindande verkan för det allmänna och kan följaktligen inte ligga till grund för några individuella rättigheter (prop. 1975/76:209 s. 128 och prop. 2009/10:80 s. 173). I 2 kap. regeringsformen finns bestämmelser som skyddar enskildas integritet i en vidare mening. Enligt 2 kap. 6 § andra stycket regeringsformen är var

[7] SOU 2016:65 s. 34, med vidare hänvisning till bl.a. Integritetsutredningen i SOU 2002:18 s. 52 f. och Integritetsskyddskommittén i SOU 2007:22 s. 53 f.

och en – utöver vad som anges i första stycket i paragrafen om bl.a. påtvingade kroppsliga ingrepp – skyddad gentemot det allmänna mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Grundlagsskyddet omfattar enbart betydande intrång. Bestämmelsen infördes den 1 januari 2011 i syfte att stärka skyddet för den personliga integriteten. Begränsning av skyddet får enligt 2 kap. 20 § regeringsformen göras i lag. Det får endast ske för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. Begränsningen får inte gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den och inte heller sträcka sig så långt att den utgör ett hot mot den fria åsiktsbildningen. Begränsningen får inte heller göras enbart på grund av politisk, religiös, kulturell eller annan sådan åskådning (2 kap. 21 §).

I förarbetena till ändringen i 2 kap. 6 § framhålls att det är naturligt att det läggs stor vikt vid uppgifternas karaktär vid bedömningen av hur ingripande intrånget i den personliga integriteten kan anses vara i samband med insamling, lagring och bearbetning eller utlämnande av uppgifter om enskildas personliga förhållanden. Ju känsligare uppgifterna är, desto mer ingripande anses det allmännas hantering av uppgifterna normalt vara. Även hantering av ett fåtal uppgifter kan med andra ord innebära ett betydande intrång i den personliga integriteten om uppgifterna är av mycket känslig karaktär. Vid bedömningen av intrångets karaktär är det också naturligt att stor vikt läggs vid ändamålet med behandlingen. En hantering som syftar till att utreda brott kan enligt förarbetena normalt anses vara mer känslig än t.ex. en hantering som uteslutande sker för att ge en myndighet underlag för förbättringar av kvaliteten i handläggningen. Mängden uppgifter kan också vara en betydelsefull faktor i sammanhanget (prop. 2009/10:80 s. 183).

4.3.3 Personuppgiftslagen

Personuppgiftslagen upphävdes i samband med dataskyddslagens ikraftträdande. Enligt övergångsbestämmelse 2 till dataskyddslagen ska personuppgiftslagen bl.a. fortsätta att gälla i sådan verksamhet hos Försvarsmakten och Försvarets radioanstalt som inte omfattas av unionsrätten. Den behandling av personuppgifter som omfattas

av lagen om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelse- och militära säkerhetstjänst och lagen om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet är undantagen dataskyddslagen på sätt som beskrivs närmare i avsnitt 4.3.3. Mot denna bakgrund följer här en redogörelse för personuppgiftslagens innehåll.

Personuppgiftslagen innehåller generella regler för all behandling av personuppgifter, dvs. enligt lagen all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet. Begreppet behandling av personuppgifter omfattar i stort sett allt man kan göra med sådana uppgifter, t.ex. att samla in, söka, bevara eller sprida uppgifter (3 §).

Personuppgiftslagen tillämpas på helt eller delvis automatiserad behandling av personuppgifter men är även tillämplig på manuell behandling av personuppgifter som ingår, eller är avsedda att ingå, i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier (5 §).

Personuppgiftslagen uppställer vissa grundläggande krav för behandling av personuppgifter; bl.a. laglig behandling, på ett korrekt sätt och i enlighet med god sed (9 §). Därtill får personuppgifter bara samlas in för särskilda, uttryckligt angivna och berättigade ändamål. Det innebär att ändamålen med en behandling av personuppgifter måste bestämmas redan när uppgifterna samlas in. Personuppgifterna får sedan inte behandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in. Denna s.k. finalitetsprincip är av central betydelse vid behandling av personuppgifter och innebär att en prövning måste göras av om eventuella nya ändamål med behandlingen är oförenliga med de ursprungligt angivna ändamålen.

Personuppgiftslagen förbjuder behandling av känsliga personuppgifter; uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening och uppgifter som rör hälsa eller sexualliv. Sådana uppgifter får emellertid behandlas i enlighet med vissa särskilt angivna undantag, bl.a. uttryckligt samtycke från den registrerade. Regeringen, eller den myndighet regeringen bestämmer, får föreskriva ytterligare undantag från förbudet om det behövs med hänsyn till ett viktigt allmänt intresse (13, 15 och 20 §§).

Datainspektionen är tillsynsmyndighet enligt personuppgiftslagen (2 § personuppgiftsförordningen [1998:1191]).

Även om personuppgiftslagen härrör ur ett EU-direktiv är lagen, som den formulerats i svensk rätt, inte begränsad till vissa områden, utan är generellt tillämplig och omfattar således även personuppgiftsbehandling utanför unionsrätten. Särreglering i lag eller förordning gäller emellertid framför bestämmelserna i personuppgiftslagen (2 §). Sådan särreglering får inte stå i strid med dataskyddskonventionen.

Enligt 22 § personuppgiftslagen får uppgifter om personnummer eller samordningsnummer behandlas utan samtycke bara när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl. Bestämmelser om i vilka fall information om behandling av personuppgifter ska lämnas till den enskilde finns i 23–27 §§. Bestämmelserna om informationsplikt gäller inte om sekretess eller tystnadsplikt är föreskriven för uppgifterna. På begäran av den registrerade är den personuppgiftsansvarige skyldig att snarast rätta, blockera eller utplåna sådana personuppgifter som inte har behandlats i enlighet med personuppgiftslagen eller föreskrifter som har utfärdats med stöd av lagen (28 §). Om felaktiga uppgifter har lämnats ut till tredje man är den personuppgiftsansvarige i vissa fall skyldig att underrätta denne om rättelsen. Det ska ske om den registrerade begär det eller om mera betydande skada eller olägenhet för den registrerade skulle kunna undvikas genom en underrättelse. Tredje man behöver dock inte underrättas om det visar sig vara omöjligt eller skulle innebära en oproportionerligt stor arbetsinsats. För att säkerställa en hög säkerhetsnivå vid behandling av personuppgifter finns särskilda bestämmelser om detta i 30–32 §§.

Det är förbjudet att föra över personuppgifter till tredje land, dvs. en stat utanför EU eller EES, som inte har en adekvat nivå för skyddet av personuppgifterna (33 §). Förbudet gäller i princip alla personuppgifter. Under vissa förutsättningar är det dock tillåtet att föra över uppgifter till tredje land under förutsättning att den registrerade antingen gett sitt samtycke eller överföringen är nödvändig bl.a. för att rättsliga anspråk ska kunna fastställas, göras gällande eller försvaras, eller för att vitala intressen för den registrerade ska kunna skyddas (34 §). Det är också tillåtet att föra över personuppgifter för

användning enbart i en stat som har anslutit sig till dataskyddskonventionen. Regeringen får meddela föreskrifter om ytterligare undantag från förbudet mot överföring (35 §).

Behandling av personuppgifter ska som huvudregel anmälas till Datainspektionen i dess egenskap av tillsynsmyndighet. En anmälan behöver dock inte göras om det finns ett personuppgiftsombud eller om något av de i personuppgiftsförordningen föreskrivna undantagen är tillämpligt (36 och 37 §§).

Vidare finns det i personuppgiftslagen bestämmelser om personuppgiftsombud (38–40 §§), krav på förhandskontroll i vissa fall (41 §), allmän informationsskyldighet (42 §) och tillsynsmyndighetens befogenheter (43–47 §§). Det finns också bestämmelser om skadestånd och straff (48–49 §§) samt om överklagande (51–53 §§).

4.3.4 Särskilda registerförfattningar

Syftet med särskilda registerförfattningar är att anpassa skyddet för enskildas personliga integritet vid myndigheters personuppgiftsbehandling när det finns ett behov av att avvika från eller komplettera personuppgiftslagens bestämmelser. Inom olika verksamhetsområden i den offentliga sektorn är det inte ovanligt att myndigheter har särskilda behov som tillgodoses genom att i en registerförfattning ge ett anpassat integritetsskydd vid myndighetens hantering av personuppgifter. Riksdagen har sedan lång tid tillbaka också gett uttryck för uppfattningen att myndighetsregister med ett stort antal registrerade och med ett känsligt innehåll ska regleras särskilt i lag (prop. 1990/91:60 s. 50, KU 1990/91:11 s. 11 och rskr. 1990/91:160). Det finns ett stort antal lagar om behandling av personuppgifter som gäller i viss verksamhet eller för ett visst register. Exempel på sådana särskilda registerförfattningar är lagen (1998:938) om behandling av personuppgifter om totalförsvarspliktiga, patientdatalagen (2008:355) och polisdatalagen (2010:361).

Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst och Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet regleras i särskilda författningar, vilket beskrivs närmare i avsnitt 5.

4.3.5 Offentlighets- och sekretesslagen

Offentlighets- och sekretesslagen (2009:400) innehåller ett flertal bestämmelser om sekretess till skydd för uppgifter om enskildas personliga förhållanden, vilka också medför ett skydd för enskildas personliga integritet. Av 21 kap. 7 § framgår att sekretess gäller för en personuppgift om det kan antas att uppgiften efter ett utlämnande kommer att behandlas i strid med dataskyddsförordningen eller dataskyddslagen. Sekretessprövningen gäller således den behandling som kommer att ske efter ett eventuellt utlämnande. Utlämnanden till utländska mottagare som omfattas av dataskyddsförordningens tillämpningsområde omfattas också av sekretessbestämmelsen (prop. 2017/18:105 s. 210).

5 Regleringen av personuppgiftsbehandling vid Försvarsmakten och Försvarets radioanstalt

5.1.1 Allmänt

Försvarsmaktens personuppgiftsbehandling inom ramen för försvarsunderrättelseverksamheten och den militära säkerhetstjänsten regleras i lagen (2007:258) och förordningen (2007:260) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst (FM-PuL och FM-PuF). Regleringen är uppbyggd på samma sätt för Försvarets radioanstalts behandling av personuppgifter som sker med stöd av lagen (2007:259) och förordningen (2007:261) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet (FRA-PuL och FRA-PuF).

FM-PuL och FRA-PuL gäller vid behandling av personuppgifter inom respektive lags tillämpningsområden 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. Båda lagarna syftar också till att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter inom lagarnas respektive tillämpningsområden (1 kap. 1 och 2 §§ FM-PuL och FRA-PuL).

Propositionen 2006/07:46 ligger till grund för både FM-PuL och FRA-PuL och merparten av bestämmelserna för Försvarsmaktens och Försvarets radioanstalts personuppgiftsbehandling är utformade på samma sätt i de båda lagarna. Vissa bestämmelser som gäller för den ena myndigheten saknar emellertid motsvarighet i den andra

lagen. Dessa bestämmelser redovisas i förekommande fall separat för respektive myndighet.

FM-PuL och FRA-PuL är båda självständiga och heltäckande regleringar som ersätter personuppgiftslagen fullt ut inom sina respektive tillämpningsområden (1 kap. 1 § andra stycket FM-PuL och FRA-PuL).

Försvarsmakten respektive Försvarets radioanstalt är personuppgiftsansvariga för den behandling av personuppgifter som myndigheterna utför (1 kap. 5 § FM-PuL och FRA-PuL).

När det gäller Försvarets radioanstalt innehåller även lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet vissa bestämmelser om personuppgiftsbehandling, t.ex. användningen av sökbegrepp och förstöringsskyldighet. Av lagen framgår bl.a. att inhämtning av signaler i tråd ska ske automatiserat och att sådan inhämtning endast får avse signaler som identifierats genom sökbegrepp. Upptagning eller uppteckning av uppgifter som inhämtats enligt lagen om signalspaning i försvarsunderrättelseverksamhet ska omgående förstöras om innehållet bl.a. berör en viss fysisk person och har bedömts sakna betydelse för försvarsunderrättelseverksamheten (1 och 7 §§).

För Försvarsmaktens och Försvarets radioanstalts övriga personuppgiftsbehandling som inte omfattas av FM-PuL eller FRA-PuL gäller personuppgiftslagen (1998:204). Som nämnts i avsnitt 4.2.2 gäller detta sedan 25 maj 2018 för sådan verksamhet som inte omfattas av unionsrätten.

5.1.2 När behandling av personuppgifter är tillåten

Myndigheternas försvarsunderrättelseverksamhet

Av 1 kap. 8 § FM-PuL och FRA-PuL framgår att personuppgifter får behandlas i respektive myndighets försvarsunderrättelseverksamhet om det är nödvändigt för att bedriva den verksamhet som anges i lagen (2000:130) om försvarsunderrättelseverksamhet. Regeringen konstaterade att försvarsunderrättelseverksamheten är av sådan art att det inte ansetts möjligt att i lagform reglera den i detalj. Utöver bestämmelserna i lagen och förordningen om försvarsunderrättelseverksamhet styrs emellertid verksamheten även av regeringens inriktning, vilken ytterligare avgränsar de ändamål för vilka verksamheten

får bedrivas. Försvarsmakten och Försvarets radioanstalt producerar dessutom interna styrdokument där en ytterligare precisering i förhållande till regeringens inriktning görs. På detta sätt bestämmer myndigheterna närmare ändamålen för verksamheten – och därmed ramen för behandlingen av personuppgifter – i enlighet med vad uppgiften som personuppgiftsansvarig ålägger myndigheten (se prop. 2006/07:46 s. 64, 65 och 67). Som beskrivits i avsnitt 3.3.5 anger lagen om signalspaning i försvarsunderrättelseverksamhet för vilka syften signalspaning får ske.

Av 1 kap. 8 § andra stycket FM-PuL och FRA-PuL framgår att uppgifter om en person endast får behandlas om personen också har anknytning till en preciserad inriktning för försvarsunderrättelseverksamheten och behandlingen är nödvändig för att fullfölja den inriktningen. Med preciserad inriktning avses de interna styrdokument som myndigheterna fastställer för närmare avgränsning av verksamheten. Vilken grad av anknytning en person ska ha till en preciserad inriktning för att behandling av uppgifter om honom eller henne ska kunna anses godtagbar, måste med hänsyn till verksamheternas 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 (se prop. 2006/07:46 s. 65 och 67).

Tillgången till personuppgifter ska alltid begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter (1 kap. 16 § FM-PuL och FRA-PuL).

Försvarsmaktens militära säkerhetstjänst

Personuppgifter får enligt 1 kap. 9 § FM-PuL behandlas i den militära säkerhetstjänstens verksamhet för att upptäcka, förebygga och avvärja säkerhetshotande verksamhet som riktar sig mot Försvarsmakten och dess säkerhetsintressen, om det är nödvändigt för att

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

För de ändamål som anges i 1 kap. 9 § FM-PuL får uppgifter om en person enligt 1 kap. 10 § behandlas endast om uppgifterna ger grundad anledning att anta att personen

1. har utövat eller kan komma att utöva verksamhet som innefattar brott som kan hota rikets säkerhet eller terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott eller motsvarande brottslighet enligt tidigare lagstiftning,
2. har utövat eller kan komma att utöva underrättelseverksamhet riktad mot Försvarsmakten och dess säkerhetsintressen,
3. utövar annan säkerhetshotande verksamhet än som avses i 1 och som innefattar brott eller åsidosättande av åligganden i anställning hos Försvarsmakten, och det finns särskilda skäl till att uppgiften skall behandlas,
4. har lämnat uppgifter om säkerhetshotande verksamhet och personuppgifterna är nödvändiga för att bedöma personens trovärdighet, eller
5. att uppgifterna avser information som har framkommit i samband med att en person har genomgått registerkontroll eller särskild personutredning enligt säkerhetsskyddslagen (1996:627).

Av 1 kap. 11 § FM-PuL framgår när personuppgifter som ingår i eller har uppkommit i samband med användning av totalförsvarets telekommunikations- och informationssystem får behandlas i förhållande till de nämnda villkoren i 10 §.

Liksom inom försvarsunderrättelseverksamheten ska tillgången till personuppgifter alltid begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter.

Försvarets radioanstalts utvecklingsverksamhet

Personuppgifter får enligt 1 kap. 9 § FRA-PuL behandlas av Försvarets radioanstalt om det är nödvändigt för att

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

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

Därutöver får personuppgifter behandlas av Försvarets radioanstalt om det är nödvändigt för att biträda andra myndigheter vid värdering utveckling, anskaffning och drift av signalspaningssystem (1 kap. 10 § FRA-PuL).

5.1.3 Känsliga personuppgifter

Försvarsmakten och Försvarets radioanstalt får inte behandla personuppgifter enbart på grund av vad som är känt om en persons ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexualliv (känsliga personuppgifter). Om myndigheterna behandlar uppgifter om en person på annan grund får de emellertid komplettera (dvs. behandla) dessa uppgifter med känsliga personuppgifter om det är absolut nödvändigt för ändamålet med behandlingen (1 kap. 12 § FM-PuL och 1 kap. 11 § FRA-PuL).

5.1.4 Behandling av personuppgifter hos Försvarets radioanstalt i vissa fall

Försvarets radioanstalt tillförs en mycket stor mängd obearbetad information som inhämtats genom signalspaning. Informationen är ofta såväl krypterad som avfattad på ett främmande språk. Det är först sedan de inhämtade signalerna har lagrats och därefter kryptoforcerats och översatts, som informationen kan tas fram i klartext eller sändningarnas innehåll kan beskrivas. Det är alltså först då det är utrett om det insamlade materialet innehåller personuppgifter och om det även är fråga om t.ex. känsliga personuppgifter. 1 kap. 13 § FRA-PuL ges Försvarets radioanstalt ett stöd för nu beskrivna åtgärder inte strider mot lagen i det skede av behandlingen då det ännu inte kunnat fastställas om informationen innehåller personuppgifter. Så snart det kunnat fastställas om informationen innehåller personuppgifter måste vidare behandling av sådana uppgifter ske i överensstämmelse med vad som anges i lagen.

5.1.5 Uppgiftssamlingar

Försvarsmakten och Försvarets radioanstalt får behandla personuppgifter i uppgiftssamlingar (1 kap. 7 § FM-PuL och FRA-PuL).

Av FM-PuF och FRA-PuF framgår vilka uppgiftssamlingar som får finnas hos Försvarsmakten respektive Försvarets radioanstalt samt vilka uppgifter som får behandlas i varje samling.

Uppgiftssamlingar hos Försvarsmakten

Hos Försvarsmakten får det finnas uppgiftssamlingar för försvarsunderrättelseverksamhet. Dessa uppgiftssamlingar får endast innehålla identifieringsuppgifter, uppgifter om de omständigheter och händelser som ger anledning att anta att den registrerade har betydelse för försvarsunderrättelseverksamheten samt upplysningar om varifrån den registrerade uppgiften kommer och om en uppgiftslämnares trovärdighet. Det framgår vidare att uppgiftssamlingarna endast får innehålla uppgifter som behövs för att Försvarsmakten ska kunna fullgöra uppgifter enligt lagen (2000:130) om försvarsunderrättelseverksamhet (2 § FM-PuF).

Försvarsmakten får även inom ramen för den militära säkerhetstjänsten behandla personuppgifter i uppgiftssamlingar för:

1. Säkerhetsunderrättelsetjänst (3 §). Uppgiftssamlingarna får endast innehålla uppgifter som är nödvändiga för att upptäcka och klarlägga säkerhetshotande verksamhet som riktas mot Försvarsmakten och dess säkerhetsintressen.

2. Säkerhetsskyddstjänst (4 §). Uppgiftssamlingarna får endast innehålla uppgifter som är nödvändiga för att förebygga och avvärja säkerhetshotande verksamhet som riktas mot Försvarsmakten och dess säkerhetsintressen.

3. Signalkontroll (5 §). Uppgiftssamlingarna får endast innehålla uppgifter som är nödvändiga för att förhindra obehörig insyn i och påverkan av totalförsvarets telekommunikations- och informationssystem.

Bestämmelserna i 3–5 §§ innehåller även vissa särskilda regler om gallring av uppgifter i uppgiftssamlingarna. Bestämmelser om gallring redogörs för i avsnitt 5.1.12.

Uppgiftssamlingar hos Försvarets radioanstalt

Hos Försvarets radioanstalt får det enligt FRA-PuF finnas uppgiftssamlingar för:

1. Råmaterial (2 §). Uppgiftssamlingarna får endast innehålla obearbetat och automatiskt bearbetat material som har inhämtats i försvarsunderrättelseverksamheten och utvecklingsverksamheten.
2. Analyser (3 §). Uppgiftssamlingarna får endast innehålla analysresultat samt bearbetnings- och rapportunderlag.
3. Underrättelser (4 §). Uppgiftssamlingarna får endast innehålla färdiga underrättelserapporter.
4. Information om signalmiljön (5 §). Uppgiftssamlingarna får endast innehålla information och tekniska parametrar som rör signalmiljön.
5. Information om företeelser mot vilka signalspaningen inriktas (6 §). Uppgiftssamlingarna får endast innehålla sådan information om signalspaningsobjekt som är nödvändig för att verkställa inriktningar av signalspaningen.
6. Information om teknik- och metodikutveckling (6 a §). Uppgiftssamlingarna får endast innehålla information och tekniska parametrar som rör teknik- och metodikutvecklingen.
7. Information om signalskydd (6 b §). Uppgiftssamlingarna får endast innehålla information och tekniska parametrar som rör signalskyddet.

Bestämmelserna i 2, 5 och 6 §§ innehåller även vissa särskilda regler om hur länge personuppgifterna får behandlas. Bestämmelser om gallring redogörs för i avsnitt 5.1.12.

5.1.6 Vidarebehandling av personuppgifter för vissa andra ändamål

Vidarebehandling av personuppgifter för vissa andra ändamål än de ursprungliga, s.k. sekundära ändamål, får göras med stöd av 1 kap. 6 § 4 p FM-PuL och FRA-PuL. Bestämmelserna ger möjlighet att fortsatt behandla insamlade uppgifter så länge personuppgifterna inte

behandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in (finalitetsprincipen).

5.1.7 Elektroniskt utlämnande av och direktåtkomst till personuppgifter

Utlämnande på medium för automatiserad behandling

Försvarsmakten och Försvarets radioanstalt får endast lämna ut enstaka personuppgifter på medium för automatiserad behandling, om inte regeringen har meddelat föreskrifter eller i ett enskilt fall beslutat om att uppgifter får lämnas ut på sådant medium även i andra fall (1 kap. 14 § FM-PuL och FRA-PuL). Av FM-PuF och FRA-PuF framgår att utlämnande på sådant medium får ske avseende fler än enstaka uppgifter om uppgifterna lämnas ut till en annan statlig myndighet.

Direktåtkomst

Bestämmelser om direktåtkomst regleras i 1 kap. 15 § FM-PuL och FRA-PuL och är ändrad sedan den 1 mars 2018. Innan ändringen fick regeringen meddela föreskrifter om vilka myndigheter som får ha direktåtkomst till Försvarsmaktens och Försvarets radioanstalts uppgiftssamlingar. Regeringen föreslog i prop. 2017/18:36 att Säkerhetspolisen, Försvarets radioanstalt och Försvarsmakten, inom ramen för samarbetet vid Nationellt centrum för terrorhotbedömning (NCT), ska få lämna ut uppgifter till varandra elektroniskt genom direktåtkomst. Regeringens förslag innehöll ändringar i FM-PuL, FRA-PuL och polisdatalagen (2010:361). När det gäller valet av regleringsform fann regeringen att ett möjliggörande av direktåtkomst som form för utlämnande av uppgifter mellan ovan nämnda myndigheter inom ramen för NCT-samarbetet inte medför att det uppkommer ett sådant betydande intrång i enskildas personliga integritet som innebär övervakning eller kartläggning i den mening som avses i 2 kap. 6 § andra stycket regeringsformen. Regeringen ansåg emellertid ändå att det i det aktuella fallet vara mest ändamålsenligt att reglera direktåtkomsten i lag, främst mot bakgrund av den känsliga verksamhet som myndigheterna inom NCT-samarbetet bedriver samt då utlämnandet förutsätter att sekretessbrytande bestämmelser

om uppgiftsskyldighet införs. Regeringen beaktade också det faktum att Säkerhetspolisens utlämnande av uppgifter genom direktåtkomst föreslogs regleras i lag (prop. 2017/18:36 s. 27–28).

Riksdagen antog den 24 januari 2018 regeringens proposition och lagändringarna trädde i kraft den 1 mars 2018. Det innebär att Säkerhetspolisen, Försvarets radioanstalt och Försvarsmakten, inom ramen för samarbetet vid NCT, får lämna ut uppgifter till varandra elektroniskt genom direktåtkomst till uppgifter som behövs för att kunna göra bedömningar på strategisk nivå av terrorhotet mot Sverige och mot svenska intressen. Direktåtkomsten innebär att myndigheterna kan dela information digitalt, i stället för som tidigare i pappersformat. Nya sekretessbrytande bestämmelser i form av uppgiftsskyldigheter möjliggör utlämnandet mellan myndigheterna (1 kap. 15 a § FM-PuL och FRA-PuL). Direktåtkomsten innebär ett effektivare arbetssätt för de tre myndigheterna, men omfattar inte fler uppgifter än vad som gällde innan lagändringarna. För övriga situationer av direktåtkomst gäller alltjämt att regeringen får meddela föreskrifter om vilka myndigheter som får ha sådan åtkomst till Försvarsmaktens och Försvarets radioanstalts uppgiftssamlingar. Regeringen, eller den myndighet som regeringen bestämmer, meddelar också de ytterligare föreskrifter eller beslut i enskilda fall om omfattningen av direktåtkomsten som behövs. Det framgår exempelvis av FM-PuF och FRA-PuF att de båda myndigheterna får ha direktåtkomst till uppgifter i uppgiftssamlingar för försvarsunderrättelseverksamhet hos den andra myndigheten i den omfattning som den personuppgiftsansvariga myndigheten beslutar.

Överföring av personuppgifter till andra länder

Av 1 kap. 17 § FM-PuL och FRA-PuL följer att personuppgifter som behandlas med stöd av respektive lag får föras över till andra länder eller mellanfolkliga organisationer endast om sekretess inte hindrar det och det är nödvändigt för att Försvarsmakten eller Försvarets radioanstalt ska kunna fullgöra sina uppgifter inom ramen för det internationella försvarsunderrättelse- och säkerhetssamarbetet, om inte regeringen har meddelat föreskrifter eller i ett enskilt fall beslutat om att överföring får ske även i andra fall då det är nödvändigt för Försvarsmaktens eller Försvarets radioanstalts verksamheter.

5.1.8 Information till den enskilde, rättelse och skadestånd

Information till den enskilde

Försvarsmakten och Försvarets radioanstalt är enligt 2 kap. FM-PuL och FRA-PuL skyldiga att till var och en som ansöker om det en gång per kalenderår gratis lämna besked om huruvida personuppgifter som rör den sökande behandlas eller inte. Behandlas sådana uppgifter ska skriftlig information lämnas också om vilka uppgifter om den sökande som behandlas, varifrån dessa uppgifter har hämtats, ändamålen med behandlingen, och till vilka mottagare eller kategorier av mottagare som uppgifterna lämnas ut. Sådan information behöver inte lämnas om personuppgifter i löpande text som inte fått sin slutliga utformning när ansökan gjordes eller som utgör minnesanteckning eller liknande. Informationen ska lämnas inom en månad från ansökan, eller inom fyra månader om det finns särskilda skäl.

Om uppgifter om en person har samlats in i den militära säkerhetstjänsten från personen själv ska Försvarsmakten dessutom i samband med insamlingen självmant lämna den registrerade viss information om behandlingen av uppgifterna, bl.a. ändamålet med behandlingen och information om mottagarna av uppgifterna. Sådan information behöver emellertid inte lämnas om sådant som den registrerade redan känner till.

Om det vid signalspaning har använts sökbegrepp som är direkt hänförliga till en viss fysisk person ska Försvarets radioanstalt underrätta personen om detta enligt lagen om signalspaning i försvarsunderrättelseverksamhet.

De skyldigheter om informationsgivning och underrättelse som nämnts ovan gäller inte i den utsträckning uppgifterna omfattas av sekretess.

Rättelse

Försvarsmakten och Försvarets radioanstalt är skyldiga att på begäran av en registrerad snarast rätta, blockera eller utplåna sådana personuppgifter som inte har behandlats i enlighet med FM-PuL eller FRA-PuL, eller föreskrifter som meddelats med stöd av dessa lagar. Försvarsmakten och Försvarets radioanstalt ska 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 inte lämnas, om detta är omöjligt eller skulle innebära en oproportionerligt stor arbetsinsats (2 kap. 5 § FM-PuL och 2 kap. 4 § FRA-PuL).

Motsvarande bestämmelse finns i personuppgiftslagen. Att en personuppgift rättas innebär att den ersätts eller kompletteras med korrekta uppgifter. Med blockering avses en åtgärd som vidtas för att personuppgifter ska vara förknippade med information om att de är spärrade och om anledningen till spärren. Att en uppgift utplånas innebär att den förstörs så att den inte kan återskapas. Bestämmelsen omfattar inte behandling av uppgifter avseende juridiska personer (se prop. 2006/07:46 s. 90).

Skadestånd

Staten ska ersätta den registrerade för skada och kränkning av den personliga integriteten som en behandling av personuppgifter i strid med 2 kap. 6 § FM-PuL och 2 kap. 5 § FRA-PuL eller föreskrifter som har meddelats med stöd av lagarna har orsakat. Ersättningsskyldigheten kan i den utsträckning det är skäligt jämkas, om Försvarsmakten respektive Försvarets radioanstalt visar att felet inte berodde på myndigheten.

Anspråk på ersättning med stöd av 2 kap. 6 § FM-PuL och 2 kap. 5 § FRA-PuL riktas mot staten och handläggs av Justitiekanslern (3 § förordningen [1995:1301] om handläggning av skadeståndsanspråk mot staten). Justitiekanslern får besluta att den myndighet som är berörd i ett skaderegleringsärende eller en rättegång ska ansvara för att bl.a. ersättningsbelopp betalas ut till motparten (2 a § förordningen [1975:1345] med instruktion för Justitiekanslern).

5.1.9 Säkerheten vid behandling

I tredje kapitlet i FM-PuL och FRA-PuL anges vad som krävs för att ett personuppgiftsbiträde eller annan person som arbetar under biträdet eller Försvarsmaktens alternativt Försvarets radioanstalts ledning ska få behandla personuppgifter. Vidare tydliggörs att Försvarsmakten och Försvarets radioanstalt ska vidta lämpliga tekniska

och organisatoriska åtgärder för att skydda de personuppgifter som behandlas av myndigheterna eller av ett personuppgiftsbiträde som myndigheterna anlitat.

5.1.10 Personuppgiftsombud

Av 4 kap. FM-PuL och FRA-PuL framgår att Försvarsmakten och Försvarets radioanstalt ska utse ett eller flera personuppgiftsombud och anmäla dessa till tillsynsmyndigheten. Även ett entledigande av ett personuppgiftsombud ska anmälas till tillsynsmyndigheten. Personuppgiftsombudet ska ha till uppgift att självständigt se till att den behandlande myndigheten 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 den behandlande myndigheten bryter mot de bestämmelser som gäller för behandlingen av personuppgifter och vidtas inte rättelse så snart det kan ske efter påpekande, ska personuppgiftsombudet anmäla förhållandet till tillsynsmyndigheten. Personuppgiftsombudet ska även i övrigt samråda med tillsynsmyndigheten vid tveksamhet om hur de bestämmelser som gäller för behandlingen av personuppgifter ska tillämpas.

Personuppgiftsombudets uppgifter omfattar även att föra förteckningar över de behandlingar som Försvarsmakten och Försvarets radioanstalt genomför och som är helt eller delvis automatiserade. För Försvarsmakten ska separata förteckningar föras för försvarsunderrättelseverksamheten och den militära säkerhetstjänsten. Regeringen, eller den myndighet som regeringen bestämmer, meddelar föreskrifter om vad förteckningarna ska innehålla.

Personuppgiftsombudet ska också hjälpa registrerade att få rättelse när det finns anledning att misstänka att behandlade personuppgifter är felaktiga eller ofullständiga.

5.1.11 Tillsyn och kontroll

Datainspektionen

Datainspektionen är tillsynsmyndighet för den personuppgiftsbehandling som sker enligt FM-PuL och FRA-PuL, och tillsynen regleras i lagarnas femte kapitel.

Tillsynsmyndigheten har rätt att för sin tillsyn på begäran få tillgång till de personuppgifter som behandlas, upplysningar om och dokumentation av behandlingen av personuppgifter och säkerheten vid denna och 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, ska myndigheten genom påpekanden eller liknande förfaranden försöka åstadkomma rättelse. Tillsynsmyndigheten får hos förvaltningsrätten inom vars domkrets tillsynsmyndigheten är belägen ansöka om att sådana personuppgifter som har behandlats på ett olagligt sätt ska utplånas, om ett beslut om utplånande inte skulle vara oskäligt.

Statens inspektion för försvarsunderrättelseverksamheten

Statens inspektion för försvarsunderrättelseverksamheten (Siun) är ansvarig kontrollmyndighet för försvarsunderrättelseverksamheten enligt lagen om försvarsunderrättelseverksamhet och för signalspaning i sådan verksamhet enligt lagen om signalspaning i försvarsunderrättelseverksamhet. Siun har även till uppgift att granska behandlingen av uppgifter enligt FM-PuL och FRA-PuL, vilket framgår av 3 § förordningen (2009:969) med instruktion för Statens inspektion för försvarsunderrättelseverksamheten.

5.1.12 Gallring av personuppgifter

Gallring av personuppgifter hos Försvarsmakten

Vilka uppgiftssamlingar som finns hos Försvarsmakten behandlas ovan under avsnitt 5.1.5.

Enligt huvudregeln i 6 kap. 1 § FM-PuL ska personuppgifter hos Försvarsmakten gallras så snart uppgifterna inte längre behövs för

det ändamål för vilket de behandlas. Detta gäller dock inte, som angetts ovan, behandling av personuppgifter i samband med de interna och administrativa åtgärder som kan förekomma i myndighetens verksamhet.

För Försvarsmakten finns det i 3–5 §§ FM-PuF preciserade gallringsbestämmelser för uppgifter som behandlas i olika uppgiftssamlingar.

Personuppgifter i en uppgiftssamling för säkerhetsunderrättelsetjänst eller i en uppgiftssamling för säkerhetsskyddstjänst ska gallras senast vid utgången av det tionde året efter det att behandlingen påbörjades, om inte Försvarsmakten dessförinnan har beslutat att uppgifterna ska bevaras därför att de fortfarande behövs för det ändamål för vilket de behandlas. Om uppgifter bevaras med stöd av ett sådant beslut ska de gallras eller frågan om bevarande prövas på nytt senast vid utgången av det tionde året efter beslutet. Personuppgifter i en uppgiftssamling för

Personuppgifter i en uppgiftssamling för signalkontroll ska gallras senast ett år efter det att behandlingen av uppgifterna påbörjades.

Några sådana preciserade gallringsbestämmelser finns inte när det gäller uppgifter som behandlas i en uppgiftssamling för försvarsunderrättelseverksamhet, varför det beträffande dessa uppgifter är huvudregeln i 6 kap. 1 § FM-PuL som är tillämplig. Enligt 12 § FM-PuF får Riksarkivet meddela föreskrifter om att uppgifter och handlingar som ska gallras enligt 6 kap. 1 § FM-PuL ska bevaras.

Riksarkivet har meddelat föreskrifter som anger att vissa uppgifter som ska gallras enligt ovan ska bevaras för historiska, statistiska och vetenskapliga ändamål (se Riksarkivets föreskrifter RA-MS 2014:38). Dessa uppgifter får således inte gallras ur Försvarsmaktens arkiv.

Gallring av personuppgifter hos Försvarets radioanstalt

Vilka uppgiftssamlingar som finns hos Försvarets radioanstalt behandlas ovan under avsnitt 5.1.5.

I 6 kap. 1 § FRA-PuL föreskrivs att personuppgifter som har behandlats automatiserat ska gallras så snart uppgifterna inte längre behövs för det ändamål för vilket de behandlas, om inte regeringen eller den myndighet som regeringen bestämmer har meddelat föreskrifter eller i enskilt fall beslutat att gallring ska ske senast vid viss tidpunkt

eller att uppgifter får bevaras för historiska, statistiska eller vetenskapliga ändamål. Regeringen har gett Riksarkivet ett sådant bemyndigande att meddela föreskrifter (12 § FRA-PuF). Sådana föreskrifter får dock inte omfatta personuppgifter i uppgiftssamlingar för råmaterial.

Särskild reglering om gallring finns i 2, 5 och 6 §§ FRA-PuF när det gäller uppgiftssamlingar för råmaterial, för information om signalmiljön och för information om företeelser mot vilka signalspaningen inriktas.

Personuppgifter i en uppgiftssamling för råmaterial ska gallras senast ett år efter det att behandlingen av uppgifterna påbörjats (2 § FRA-PuF).

Personuppgifter i en uppgiftssamling om signalmiljön ska gallras senast vid utgången av det första året efter det att behandlingen av uppgifterna påbörjades, om inte Försvarets radioanstalt dessförinnan beslutat att uppgifterna ska bevaras därför att de fortfarande behövs för det ändamål för vilket de behandlas. Om uppgifterna bevaras med stöd av ett sådant beslut ska de gallras eller frågan om bevarande prövas på nytt senast vid utgången av det första året efter beslutet (5 § FRA-PuF).

Personuppgifter i en uppgiftssamling för information om företeelser mot vilka signalspaningen inriktas ska gallras senast vid utgången av det tredje året efter det att behandlingen av uppgifterna påbörjades, om inte Försvarets radioanstalt dessförinnan har beslutat att uppgifterna ska bevaras därför att de fortfarande behövs för det ändamål för vilket de behandlas. Om uppgifter bevaras med stöd av ett sådant beslut ska de gallras eller frågan om bevarande prövas på nytt senast vid utgången av det tredje året efter beslutet (6 § FRA-PuF).

Riksarkivet har beslutat att personuppgifter i Försvarets radioanstalts uppgiftssamlingar för underrättelser ska bevaras för historiska, statistiska och vetenskapliga ändamål (dnr KrA H231-2009/333). Riksarkivet har vidare beslutat att även personuppgifter i rapportunderlag i uppgiftsamlingar för analyser ska bevaras för dessa ändamål (dnr KrA H231-2017/2031).

I sammanhanget ska också nämnas de föreskrifter om förstöringsskyldighet som finns i 7 § lagen om signalspaning i försvarsunderrättelseverksamhet. Av denna bestämmelse framgår att upptagning eller

uppteckning av uppgifter som inhämtats enligt lagen omgående ska förstöras om innehållet

1. berör en viss fysisk person och har bedömts sakna betydelse för verksamhet som avses i 1 § (ändamålsparagrafen, se avsnitt 3.3.5),
2. avser uppgifter för vilka tystnadsplikt gäller enligt 3 kap. 3 § tryckfrihetsförordningen eller 2 kap. 3 § yttrandefrihetsgrundlagen, eller som omfattas av efterforskningsförbudet i 3 kap. 4 § tryckfrihetsförordningen eller 2 kap 4 § yttrandefrihetsgrundlagen,
3. omfattar uppgifter i sådana meddelanden mellan en person som är misstänkt för brott och hans eller hennes försvarare vilka skyddas enligt 27 kap. 22 § första stycket rättegångsbalken, eller
4. avser uppgifter lämnade under bikt eller enskild själavård, såvida det inte finns synnerliga skäl att behandla uppgifterna för syften som anges i 1 § andra stycket (de åtta kartläggningssyftena, se avsnitt 3.3.5).

Förstöring av upptagningar eller uppteckningar enligt 7 § lagen om signalspaning i försvarsunderrättelseverksamhet ska enligt 5 § förordningen (2008:923) om signalspaning i försvarsunderrättelseverksamhet ske på ett sådant sätt att uppgifterna inte kan återskapas.

En bestämmelse om förstöringsplikt finns också i 2 a § nämnda lag. Enligt den bestämmelsen får inhämtning inte avse signaler mellan en avsändare och mottagare som båda befinner sig i Sverige. Om sådana signaler inte kan avskiljas redan vid inhämtningen, ska upptagningen eller uppteckningen förstöras så snart det står klart att sådana signaler har inhämtats.

5.1.13 Straff och överklagande

6 kap. 2 § FM-PuL och FRA-PuL innehåller bestämmelser om straff för lämnande av osann uppgift vid vissa i bestämmelserna angivna fall och behandling av känsliga personuppgifter i strid med vad som anges i de respektive lagarna. Straffbestämmelserna infördes med beaktande av 49 § personuppgiftslagen (se prop. 2006/07:46 s. 106–107).

Av 6 kap. 3 § FM-PuL och FRA-PuL framgår att Försvarsmaktens respektive Försvarets radioanstalts beslut om viss information som ska lämnas samt om rättelse och underrättelse till tredje man får

överklagas till allmän förvaltningsdomstol. Av bestämmelsen framgår vidare att övriga beslut enligt FM-PuL och FRA-PuL inte får överklagas och att prövningstillstånd krävs vid överklagande till kammarrätten.

6 Överväganden och förslag

6.1 Allmänna utgångspunkter

6.1.1 Reglering i två nya lagar

Utredningens förslag: Två nya lagar bör reglera personuppgiftsbehandlingar inom Försvarsmakten och Försvarets radioanstalt: Lag om behandling av personuppgifter vid Försvarsmakten och Lag om behandling av personuppgifter vid Försvarets radioanstalt.

Skäl för utredningens förslag: Utredningen föreslår ett flertal förändringar av befintlig lagstiftning på området; nya författningsbestämmelser, förändringar av befintliga författningar samt nya rubriker. Målet med utredningens arbete med en ändamålsenlig lagstiftning har inte bara varit att bestämmelserna i sig ska vara anpassade efter den tekniska och legala utvecklingen, utan att lagarna, även efter de föreslagna förändringarna, ska vara överblickbara med logisk struktur och innehålla begrepp och definitioner som i möjligaste mån stämmer överens med annan lagstiftning som reglerar hantering av personuppgifter. Med beaktande av att utredningen föreslår förändringar av ett stort antal bestämmelser i lagen om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst (FM-PuL) och lagen om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet (FRA-PuL) och därtill helt nya bestämmelser till följd av vidgade tillämpningsområden bör två nya lagar ersätta de befintliga lagarna.

6.1.2 Särskild författningsreglering

Utredningens förslag: De nya lagarna ska vara heltäckande och utformas så att de exklusivt gäller på de områden som anges i respektive lag.

Skäl för utredningens förslag: Unionsrätten omfattar inte nationell säkerhet och försvar, vilket innebär att varken EU:s dataskyddsdirektiv eller dataskyddsförordning omfattar behandling av personuppgifter som rör dessa verksamheter. Den EU-rättsliga regleringen bygger emellertid på och vidareutvecklar dataskyddskonventionen som omfattar även dessa områden. Sverige är folkrättsligt bundet av konventionen med dess tilläggsprotokoll. Regleringen av Försvarsmaktens och Försvarets radioanstalts personuppgiftsbehandling får således inte strida mot bestämmelserna i dataskyddskonventionen, vilket bl.a. innebär att personuppgifter som undergår automatisk databehandling ska lagras för särskilt angivna och lagliga ändamål och inte användas på ett sätt som är oförenligt med dessa ändamål (artikel 5). Avvikelser från konventionen får endast göras om sådana avvikelser medges i nationell lagstiftning och avvikelsen är nödvändig i ett demokratiskt samhälle för att bl.a. skydda statens säkerhet (artikel 9). Det är utredningens uppfattning att det förslag till lagstiftning som här läggs fram är i överensstämmelse med konventionen.

I lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen) utvidgas tillämpningen av bestämmelserna i dataskyddsförordningen till att även gälla vid behandling av personuppgifter som utgör led i verksamhet som inte omfattas av unionsrätten (1 kap. 2 §). Detta gäller dock inte verksamhet som omfattas av FM-PuL eller FRA-PuL (1 kap. 3 §). Enligt den proposition som ligger till grund för dataskyddslagen förklarar regeringen att det med hänsyn till rikets säkerhet inte är lämpligt att dataskyddsförordningen blir tillämplig även inom de mest känsliga verksamhetsområdena innan den pågående översynen av författningarna på försvarsområdet har avslutats (prop. 2017/18:105 s. 31).

Av övergångsbestämmelserna framgår bl.a. att personuppgiftslagen ska fortsätta att gälla i sådan verksamhet hos Försvarsmakten och Försvarets radioanstalt som inte omfattas av unionsrätten och som inte heller omfattas av de särskilda lagarna om behandling av

personuppgifter i Försvarsmaktens och Försvarets radioanstalts verksamheter.

Med utgångspunkt från att ämnet för den lagstiftning som här är aktuell ligger utanför unionsrätten bör den författningsreglering som utredningen föreslår därför vara heltäckande och utformas så att den exklusivt gäller på de områden som anges i respektive lag inom det aktuella området.

Som anfördes i förarbetena till FM-PuL och FRA-PuL är de verksamheter som de båda myndigheterna bedriver och som omfattades av de då aktuella förslagen, som gällde personuppgiftsbehandling i försvarsunderrättelseverksamhet och militär säkerhetstjänst, inte identiska och verksamheterna hade endast till viss del samma syfte. Av den anledningen föranledde regleringen av respektive myndighets personuppgiftsbehandling i flera avseenden olika rättsliga lösningar (prop. 2006/07:46 s. 47). Med hänsyn till de vidgade tillämpningsområden som utredningen föreslår för regleringen av myndigheternas personuppgiftsbehandling blir detta förhållande än tydligare. Detta gäller särskilt för Försvarsmakten där tillämpningsområdet föreslås gälla myndighetens mycket omfattande huvuduppgifter.

Med beaktande av detta utformas de föreslagna lagarna så att de så långt det är möjligt och lämpligt är lika och följer strukturen i likartad lagstiftning såsom i förslaget till Säkerhetspolisens datalag.

6.2 Allmänna bestämmelser

6.2.1 Syftet med lagarna

Utredningens förslag: Syftet med lagarna ska vara att säkerställa att Försvarsmakten och Försvarets radioanstalt kan behandla personuppgifter på ett ändamålsenligt sätt och att skydda fysiska personers grundläggande fri- och rättigheter i samband med sådan behandling.

Utredningens bedömning: De föreslagna lagarna uppfyller kraven i 2 kap. 21 § regeringsformen.

Skäl för utredningens förslag: Syftet med den nuvarande lagstiftningen anges vara att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst och i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet (1 kap. 2 § FM-PuL och FRA-PuL). Av andra bestämmelser i lagarna framgår att personuppgiftsbehandlingen ska vara nödvändig (1 kap. 8 §) och att inte fler personuppgifter behandlas än som är nödvändigt med hänsyn till ändamålen med behandlingen (1 kap. 6 § 6 p FM-PuL och FRA-PuL). Enligt utredningens mening bör den särskilda bestämmelse som anger syftet med lagarna innehålla såväl kravet på ändamålsenlighet som intresset att skydda fysiska personers fri- och rättigheter.

Skäl för utredningens bedömning: I avsnitt 4.3.2 tar utredningen upp de överväganden som ligger till grund för regleringen i 2 kap. 6 § andra stycket regeringsformen om skyddet gentemot det allmänna mot betydande intrång i den personliga integriteten. Som nämns i det avsnittet får en begränsning av grundlagsskyddet göras enligt 2 kap. 20 § regeringsformen genom lag. Begränsningen får endast göras för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. Begränsningen får inte gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den och inte heller sträcka sig så långt att den utgör ett hot mot den fria åsiktsbildningen. Begränsningen får inte heller göras enbart på grund av politisk, religiös, kulturell eller annan sådan åskådning (2 kap. 21 §).

I förarbetena till bestämmelserna i 2 kap. 6 § regeringsformen angav regeringen att vid bedömningen av hur ingripande intrånget i den personliga integriteten kan anses vara i samband med insamling, lagring och bearbetning eller utlämnande av uppgifter om enskildas personliga förhållanden, är det naturligt att stor vikt läggs vid uppgifternas karaktär. Ju känsligare uppgifterna är desto mer ingripande måste det allmännas hantering av uppgifterna normalt anses vara. Även hantering av ett fåtal uppgifter kan innebära ett betydande intrång i den personliga integriteten om uppgifterna är av mycket känslig karaktär (prop. 2009/10:80 En reformerad grundlag s. 183).

Den personuppgiftsbehandling som är aktuell i detta sammanhang utgör till en del betydande intrång i den personliga integriteten

och kräver därför lagstöd. Särskilt gäller detta personuppgiftsbehandlingen i försvarsunderrättelseverksamheten. I det sammanhanget bör dock erinras att den bara får avse utländska förhållanden. De svenska försvars- och säkerhetsintressen som lagstiftningen avser att stödja har alltid varit starka och de har vuxit i styrka mot bakgrund av den säkerhetspolitiska utvecklingen. Lagstiftningens ändamål får därför anses godtagbara i ett demokratiskt samhälle och uppfyller enligt utredningen mening även i övrigt kraven i 2 kap. 21 § regeringsformen.

I tillämpningen av lagstiftningen åligger det myndigheterna att göra en avvägning mellan ändamålet med en avsedd personuppgiftsbehandling å ena sidan och graden av intrång i den personliga integriteten å den andra. Detta följer av bestämmelserna om att personuppgifter bara får behandlas för särskilda, uttryckligt angivna och berättigade ändamål. Utredningen återkommer till detta i avsnitt 6.4.1.

6.2.2 Tillämpningsområden för lagen om behandling av personuppgifter vid Försvarsmakten

Utredningens förslag: Lagen om behandling av personuppgifter vid Försvarsmakten ska gälla Försvarsmaktens behandling av personuppgifter som rör Sveriges försvar och säkerhet.

Skäl för utredningens förslag: Som framgått av avsnitt 6.1.2. faller frågor om försvar och nationell säkerhet utanför unionsrätten. Enligt dataskyddslagen ska personuppgiftslagen fortsätta att gälla i sådan verksamhet hos Försvarsmakten som inte omfattas av unionsrätten och som inte nu regleras i FM-PuL. Bakgrunden är att denna utredning bl.a. ska analysera vilket utrymme som finns för nationell reglering av den personuppgiftsbehandling i Försvarsmakten som i dag regleras i personuppgiftslagen och utifrån den analysen bedöma om behandlingen helt eller delvis bör regleras särskilt. På sikt innebär detta att det som inte regleras särskilt kommer att omfattas av dataskyddsförordningen. Det är nämligen att förvänta att övergångsregleringen kommer att ändras så att detta blir fallet.

Utredningen utgår i sin analys från de uppgifter som Försvarsmakten har.

I avsnitt 3.1 finns en utförlig beskrivning av Försvarsmaktens uppgifter. Här ska endast en kort återblick göras med betoning på myndighetens huvuduppgifter. Försvarsmakten ska upprätthålla och utveckla ett militärt försvar som ytterst kan möta ett väpnat angrepp. Grunden för Försvarsmaktens verksamhet är förmågan till väpnad strid.

Försvarsmakten ska försvara Sverige och främja svensk säkerhet samt upptäcka och avvisa kränkningar av det svenska territoriet. Försvarsmakten ska dessutom kunna värna Sveriges suveräna rättigheter och svenska intressen samt kunna förebygga och hantera konflikter och krig såväl nationellt som internationellt. Försvarsmakten ska kunna utföra sina uppgifter självständigt eller i samverkan med andra myndigheter, länder och organisationer. Försvarsmakten ska vidare med myndighetens befintliga förmåga och resurser kunna lämna stöd till civil verksamhet.

Vid höjd beredskap ska Försvarsmakten kunna krigsorganisera, mobilisera och använda alla krigsförband för att möta ett militärt hot mot Sverige och svenska intressen. Krigsförband ska kunna krigsorganiseras, även om höjd beredskap inte råder.

Enligt utredningens mening är det uppenbart att de nu beskrivna uppgifterna ligger utanför unionsrätten med undantag för uppgiften att kunna lämna stöd till civil verksamhet. Uppgifterna har också en nära beröring med Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst, verksamheter där personuppgiftsbehandlingen i dag är särreglerad genom FM-PuL och som enligt dataskyddslagen fortfarande ska var särreglerad med hänsyn till Sveriges säkerhet. Som anförs i den proposition som låg till grund för lagen om försvarsunderrättelseverksamhet, ligger det i sakens natur att försvarsunderrättelseverksamheten ska ses som ett led i Försvarsmaktens uppgifter i fred, under beredskap och i krig. I propositionen anförs vidare att försvarsunderrättelseverksamheten ska ge underlag för Försvarsmaktens beredskap, operativa verksamhet och förbandsproduktion samt för krigsorganisationens utveckling och materiella förnyelse (prop. 1999/2000:25 s. 14 f.).

Dataskyddsförordningen är, som nyss nämnts, inte tillämplig på personuppgiftsbehandling som rör försvar och nationell säkerhet. Bestämmelserna i förordningen har därför inte utformats med beaktande av försvar och nationell säkerhet. Utredningen kan heller inte se någon fördel med att låta dataskyddsförordningen helt eller delvis

bli tillämplig på Försvarsmaktens ovan beskrivna huvuduppgifter, särskilt som det i denna verksamhet finns andra verksamheter integrerade som regleras särskilt när det gäller behandlingen av personuppgifter. Tvärtom innebär detta nackdelar som kan beskrivas enligt följande.

Omvärldsbevakning behövs för att upptäcka och identifiera yttre hot mot Sverige och svenska intressen. Logistik behövs för att få fram resurser till förbandet, personaladministration för att se till att rätt personer finns på plats för att lösa uppgiften, underrättelser behövs för att lokalisera fientliga styrkor. Operationsplanering är nödvändig för att planera och genomföra en insats. Säkerhetstjänst behövs för att säkerställa att fienden inte får tillgång till operationsplaneringen och kan motverka den. Samband behövs för att uppnå en effektiv kommunikation inom förbandet och andra förband. Civil-militär samverkan är nödvändig för att undvika skador på civilbefolkning och infrastruktur. Ett internationellt samarbete är nödvändigt när det gäller försvarsunderrättelseverksamhet men också när det gäller annat internationellt försvarssamarbete för att Försvarsmakten ska få olika former av stöd från andra länder och internationella organisationer. Inom alla dessa områden hanteras personuppgifter.

I militär säkerhetstjänst och försvarsunderrättelseverksamhet tillämpas FM-PuL, men inom logistik, samband och personaladministration tillämpas personuppgiftslagen (1998:204). Omvärldsbevakning, operationsplanering, civil-militär samverkan, samt taktisk och operativ underrättelsetjänst bedrivs med stöd av antingen FM-PuL eller personuppgiftslagen beroende på vem som hanterar uppgifterna och i vilket syfte. En personuppgift kopplad till exempelvis en specifik operation kan därför behandlas med olika personuppgiftslagstiftningar i samma databehandlingssystem.

Att ha olika regleringar för behandlingen av uppgifterna komplicerar informationsutbytet mellan system och verksamheter. Det leder till att effektiviteten inom Försvarsmakten och därmed den samlade operativa effekten försämras.

Med hänsyn till Försvarsmaktens stora betydelse för Sveriges försvar och säkerhet är det enligt utredningens uppfattning viktigt att myndighetens huvuduppgifter omfattas av en svensk nationell reglering, vilket innefattar myndighetens behandling av personuppgifter i verksamhet där uppgifterna fullgörs.

En samlad reglering bedöms innebära en förenkling för Försvarsmakten och därmed i förlängningen att integritetsskyddet stärks vid myndighetens behandling av personuppgifter.

Utredningen anser alltså att den föreslagna lagen bör omfatta behandlingen av personuppgifter i Försvarsmaktens verksamhet avseende Sveriges försvar och säkerhet. I avsnitt 6.3.1 återkommer utredningen till hur detta närmare bör regleras.

6.2.3 Tillämpningsområden för lagen om behandling av personuppgifter vid Försvarets radioanstalt

Utredningens förslag: Lagen om behandling av personuppgifter vid Försvarets radioanstalt ska gälla behandling av personuppgifter i myndighetens försvarsunderrättelse- och utvecklingsverksamhet samt informationssäkerhetsverksamhet.

Skäl för utredningens förslag: Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet är till för Sveriges försvar och säkerhet och omfattas därmed inte av unionsrätten. För personuppgiftsbehandlingen i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet gäller inte den bestämmelse i dataskyddslagen som utvidgar dataskyddsförordningen tillämpningsområde (se härom avsnitt 6.1.2). Detta är ett uttryck för att denna verksamhet ligger utanför unionsrätten och att behandlingen av personuppgifter i verksamheten fortfarande ska vara särreglerad. Utredningen föreslår ingen ändring i detta avseende.

Vidgat tillämpningsområde – informationssäkerhetsverksamhet

I avsnitt 3.3.6 redovisar utredningen Försvarets radioanstalts informationssäkerhetsverksamhet. Någon särskild reglering av personuppgiftsbehandlingen i den verksamheten finns inte.

Enligt dataskyddslagen ska personuppgiftslagen fortsätta att gälla i sådan verksamhet hos Försvarets radioanstalt som inte omfattas av unionsrätten och inte heller av FRA-PuL. Bakgrunden är att denna utredning bl.a. ska analysera vilket utrymme som finns för nationell reglering av den personuppgiftsbehandling i Försvarets radioanstalt

som i dag regleras i personuppgiftslagen och utifrån den analysen bedöma om behandlingen helt eller delvis bör regleras särskilt (se härom avsnitt 6.1.2). På sikt innebär detta att det som inte regleras särskilt kommer att omfattas av dataskyddsförordningen. Som tidigare nämnts är det att förvänta att övergångsregleringen kommer att ändras så att detta blir fallet.

Syftet med informationssäkerhetsverksamheten vid Försvarets radioanstalt är att stödja verksamheter som har betydelse för Sveriges säkerhet. Den omfattas därför inte av unionsrätten. Som framgår av avsnitt 3.3.6 har informationssäkerhetsverksamheten ett nära samband med signalspaningen. Enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet får signalspaning ske i syfte att kartlägga bl.a. allvarliga yttre hot mot samhällets infrastruktur. Som utredningen utvecklar i avsnitt 3.3.6 innebär möjligheten till utbyte av information mellan signalspaningen och informationssäkerhetsverksamheten ett viktigt verktyg för att kunna upprätthålla Sveriges säkerhet.

Dataskyddsförordningen är som nämnts i avsnitt 6.1.2 inte tillämplig på försvar och nationell säkerhet och har därför inte utformats med beaktande av detta. I likhet med vad som sägs i nämnda avsnitt kan utredningen inte heller se någon fördel med att göra dataskyddsförordningen helt eller delvis tillämplig på Försvarets radioanstalts informationssäkerhetsverksamhet. Utredningen anser därför att behandlingen av personuppgifter i informationssäkerhetsverksamheten bör vara särreglerad i likhet med behandlingen av personuppgifter i försvarsunderrättelse- och utvecklingsverksamheten. Utredningen återkommer till ämnet i avsnitt 6.3.8.

Till skillnad mot Försvarsmaktens huvuduppgifter med ett flertal olika verksamheter består uppgiften för Försvarets radioanstalt av två områden: försvarsunderrättelseverksamhet och informationssäkerhetsverksamhet. Som tidigare nämnts bidrar denna skillnad till olika rättsliga lösningar för de båda myndigheterna. Det visar sig främst genom att den föreslagna lagen om behandling av personuppgifter vid Försvarsmakten kommer att avse behandlingen av sådana uppgifter rörande myndighetens personal (avsnitt 6.3.1). Något behov av en motsvarande reglering när det gäller behandlingen av personuppgifter rörande personalen vid Försvarets radioanstalt har utredningen inte funnit.

6.2.4 Behandlingar som omfattas av de nya lagarna

Utredningens förslag: De föreslagna lagarna ska gälla för sådan behandling av personuppgifter som 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.

Skäl för utredningens förslag: Bestämmelserna i 1 kap. 1 § FM-PuL och FRA-PuL gäller vid behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst och Försvarets radioanstalts försvarsunderrättelse- 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. Manuell behandling i t.ex. register omfattas alltså av lagstiftningen om uppgifterna är tillgängliga för sökning eller sammanställning enligt mer än ett kriterium. Motiven finns i prop. 2006/07:46 s. 46–47.

Utredningen anser att den nuvarande regleringen bör behållas.

6.2.5 Lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning gäller inte personuppgiftsbehandling enligt de nya lagarna

Utredningens förslag: I de föreslagna lagarna ska införas en bestämmelse med upplysning om att lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning inte gäller vid behandling av personuppgifter i verksamheter enligt respektive lag.

Skäl för utredningens förslag: Som framgår av avsnitt 6.1.2 omfattar unionsrätten inte nationell säkerhet och försvar. De föreslagna lagarna föreslås vara helt självständiga i förhållande till övrig lagstiftning på personuppgiftsområdet, bl.a. lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen). Nämnda lag innehåller en bestämmelse som anger att verksamhet som bedrivs med stöd av FM-PuL och FRA-PuL inte omfattas av lagen

(1 kap. 3 §). Detta förhållande bör även komma till uttryck i lagarna om behandlingen av personuppgifter vid Försvarsmaktens och Försvarets radioanstalt.

6.2.6 Lagarnas förhållande till annan reglering

Utredningens förslag: Bestämmelserna i de föreslagna lagarna ska inte tillämpas i den utsträckning det skulle inskränka skyldigheten enligt 2 kap. tryckfrihetsförordningen att lämna ut personuppgifter.

Skäl för utredningens förslag: 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 ska noga anges i en särskild lag eller annan lag som den särskilda lagen hänvisar till. Den särskilda lag som åsyftas är offentlighets- och sekretesslagen (2009:400). Offentlighetsprincipen innebär således att myndigheterna är skyldiga att – i den utsträckning sekretess inte hindrar det – lämna ut allmänna handlingar till den som begär det.

En bestämmelse som i klargörande syfte upplyser att lagen inte tillämpas om det skulle inskränka Försvarsmaktens respektive Försvarets radioanstalts skyldighet enligt 2 kap. TF att lämna ut personuppgifter finns i 1 kap. 3 § FM-PuL och FRA-PuL. Motiven framgår av prop. 2006/07:46 s. 49 f.

Samma skäl som tidigare gör sig fortfarande gällande och utredningen föreslår därför att även de nya lagarna ska innehålla en motsvarande upplysning. Bestämmelsen föreslås bli neutralt formulerad, men innehåller inte några förändringar i sak i förhållande till nuvarande lydelse.

6.2.7 Personuppgiftsansvar

Utredningens förslag: Försvarsmakten respektive Försvarets radioanstalt ska vara personuppgiftsansvariga för den behandling som respektive myndighet utför. Personuppgiftsansvaret omfattar all behandling av personuppgifter som utförs under myndighetens ledning eller på dess vägnar.

Skäl för utredningens förslag: Av 1 kap. 5 § i FM-PuL och FRA-PuL framgår att Försvarsmakten respektive Försvarets radioanstalt är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför. Motiven framgår av prop. 2006/07:46 s. 52 f.

Med personuppgiftsansvarig avses den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandling av personuppgifter.

Av FM-PuL och FRA-PuL framgår för vilka ändamål behandling av personuppgifter får ske. I personuppgiftsansvaret ingår att bestämma medlen för och, inom ramen för dessa ändamål, de närmare ändamålen med behandlingen av personuppgifterna. Försvarsmakten respektive Försvarets radioanstalt är personuppgiftsansvariga för den behandling av personuppgifter som utförs inom respektive myndighets verksamhet. Personuppgiftsansvaret innebär bl.a. att Försvarsmakten 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. Motsvarande bestämmelser föreslås ingå även i de nya lagarna.

6.2.8 Gemensamt personuppgiftsansvar

Utredningens förslag: Försvarsmakten och Försvarets radioanstalt får vara gemensamt personuppgiftsansvarig med annan endast i den utsträckning det följer av lag eller förordning eller om regeringen i ett enskilt fall beslutar om det.

Skäl för utredningens förslag: Begreppet gemensamt personuppgiftsansvar finns i både dataskyddsförordningen (artikel 26) och i 2016 års dataskyddsdirektiv (artikel 21). Av dataskyddsförordningen

framgår att om två eller fler personuppgiftsansvariga gemensamt fastställer ändamålen med och medlen för behandlingen ska de vara gemensamt personuppgiftsansvariga. Enligt förordningen ska gemensamt personuppgiftsansvariga under öppna former fastställa sitt respektive ansvar för att fullgöra de skyldigheter som framgår av förordningen, särskilt vad gäller utövandet av den registrerades rättigheter och sina respektive skyldigheter att tillhandahålla information, i den mån detta inte framgår av förordningen. Inom ramen för arrangemanget får en gemensam kontaktpunkt för de personuppgiftsansvariga utses. Detta arrangemang ska på lämpligt sätt återspegla de gemensamt personuppgiftsansvarigas respektive roller och förhållanden gentemot registrerade och det väsentliga innehållet i arrangemanget ska också göras tillgängligt för den registrerade. Oavsett formerna för de gemensamt personuppgiftsansvarigas arrangemang får den registrerade utöva sina rättigheter emot var och en av de personuppgiftsansvariga.

Även enligt 2016 års dataskyddsdirektiv avses att två eller flera personuppgiftsansvariga har gemensamt ansvar för registrerade uppgifter, om de gemensamt fastställer behandlingens ändamål och medel och på samma sätt som de enligt förordningen fastställer sitt respektive ansvar för regelefterlevnaden, särskilt vad gäller utövandet av den registrerades rättigheter och sina respektive skyldigheter att tillhandahålla viss information. På samma sätt som enligt dataskyddsförordningen får den registrerade utöva sina rättigheter med avseende på var och en av de personuppgiftsansvariga.

En bestämmelse om gemensamt personuppgiftsansvar finns i förslaget till Säkerhetspolisens datalag (SOU 2017:74). Enligt den får Säkerhetspolisen vara gemensamt personuppgiftsansvarig med annan i den utsträckning det följer av lag eller förordning eller om regeringen i ett enskilt fall beslutar om det (1 kap. 8 §).

Med anledning av Försvarsmaktens och Försvarets radioanstalts nära samarbete dels med varandra, dels med Säkerhetspolisen, bedömer utredningen att det bör införas en möjlighet att ha gemensamt personuppgiftsansvar.

Liksom i förslaget till Säkerhetspolisens datalag bör gemensamt personuppgiftsansvar endast få förekomma i den utsträckning det följer av lag eller förordning eller om regeringen i ett enskilt fall beslutar om det.

I den förordning som ska knyta an till lagen om behandling av personuppgifter vid Försvarsmakten bör föreskrivas att Försvarsmakten får vara gemensamt personuppgiftsansvarig med Säkerhetspolisen, Nationella operativa avdelningen i Polismyndigheten, Myndigheten för samhällsskydd och beredskap, Försvarets materielverk, Försvarets radioanstalt och Totalförsvarets rekryteringsmyndighet.

I den förordning som ska anknyta till lagen om behandling av personuppgifter vid Försvarets radioanstalt bör anges att Försvarets radioanstalt får ha gemensamt personuppgiftsansvar med Försvarsmakten och Säkerhetspolisen inom ramen för myndighetsövergripande samverkan mellan myndigheterna för att kunna kartlägga

1. yttre militära hot mot landet,
2. förutsättningar för svenskt deltagande i fredsfrämjande och humanitära insatser eller hot mot säkerheten för svenska intressen vid genomförande av sådana insatser
3. strategiska förhållanden avseende internationell terrorism som kan hota väsentliga nationella intressen,
4. allvarliga yttre hot mot samhällets infrastruktur, samt
5. främmande underrättelseverksamhet mot svenska intressen.

I förordningarna bör det vidare föreskrivas att när respektive myndighet är gemensamt personansvarig med annan ska myndigheten säkerställa att de förpliktelser var och en har i egenskap av personuppgiftsansvarig regleras i en skriftlig överenskommelse Vid en sådan överenskommelse ska respektive myndighets författningsenliga skyldigheter kvarstå. I förordningarna bör slutligen föreskrivas att den som personuppgiften rör får, trots en sådan överenskommelse, utöva sina rättigheter gentemot var och en av de personuppgiftsansvariga.

6.2.9 Uttryck i lagen

Utredningens förslag: Vissa uttryck som används i de föreslagna lagarna ska definieras.

Skäl för utredningens förslag: Sedan FM-PuL:s och FRA-PuL:s tillkomst 2007 har det skett vissa förändringar på de tekniska och legala områdena vilket har påverkat vissa begrepps innebörd. Utvecklingen innebär också att vissa begrepp har tillkommit medan andra har tagits bort eller bytts ut. Med anledning av EU:s dataskyddsförordning och de lagar och lagändringar som är en följd av 2016 års dataskyddsdirektiv förekommer vissa begrepp både i lagstiftning som faller under och utanför EU-rätten. I den mån samma begrepp används bör de i möjligaste mån ha samma betydelse även i lagstiftning som reglerar verksamhet utanför EU-rätten.

Nedan följer en genomgång av begreppens definitioner samt huruvida begreppen är nytillkomna, förändrade, oförändrade eller inte längre ska förekomma i lagtexten.

Behandling av personuppgifter

Behandling av personuppgifter definieras i FM-PuL och FRA-PuL som 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.

Utredningen föreslår att behandling av personuppgifter i de nya lagarna definieras som ”En åtgärd eller kombination av åtgärder som vidtas i fråga om personuppgifter eller uppsättningar av personuppgifter, oavsett om det görs automatiserat eller inte, t.ex. insamling, registrering, organisering, strukturering, lagring, bearbetning eller tillhandahållande på annat sätt, justering, sammanföring, begränsning ändring, framtagning, läsning, användning, utlämnande, spridning eller, radering eller förstöring.”

Den föreslagna lydelsen, som har samma lydelse som förslagen till motsvarande definitioner i Säkerhetspolisens datalag och brottsdatalagen, innebär språkliga skillnader jämfört med dataskyddsförordningen och vissa ändringar i de uppräknade exemplen jämfört med FM-PuL och FRA-PuL; återvinning, inhämtande, blockering och utplåning tas bort, medan strukturering, framtagning, läsning, justering, sammanföring, begränsning och radering tillkommer.

Beträffande begreppen radering och förstöring kan följande noteras. Radering finns med i uppräkningen i dataskyddsförordningens artikel 4 som alternativ till bl.a. förstöring, men någon närmare förklaring till vad radering innebär finns inte utöver att raderingen (enligt artikel 17) kopplas till ”rätten att bli bortglömd”. Radering/rätten att bli bortglömd antyder att radering enligt dataskyddsförordningen innebär att personuppgifterna ska raderas/tas bort permanent från alla databärare/informationssamlingar, dvs. på ett sådant sätt att informationen inte kan återskapas vid senare tillfälle (se även SOU 2017:29 s. 727 och SOU 2017:39 s. 317), dvs. samma betydelse som *utplåna* enligt FM-PuL och FRA-PuL (jfr. SOU 1997:39 s. 402 f.). Begreppet radering kan jämföras med förstöring, som är det begrepp som används i lagen om signalspaning i försvarsunderrättelseverksamhet (2 a, 7 och 10 §§). Enligt 5 § förordningen om signalspaning i försvarsunderrättelseverksamhet ska förstöring ske på ett sådant sätt att uppgifterna inte kan återskapas. Båda begreppen syftar alltså till att data ska raderas/förstöras på ett sådant sätt att den inte kan återskapas. Hur dessa processer går till får förändras i takt med den tekniska utvecklingen.

Beträffande begreppet *begränsning* kan följande noteras. Enligt 1 kap. 4 § FM-PuL och FRA PuL är *blockering* en åtgärd som vidtas för att personuppgifterna ska vara förknippade med information om att de är spärrade och om anledningen till spärren och för att personuppgifterna inte ska lämnas ut till tredje man annat än med stöd av 2 kap. TF. Definitionen stämmer väl överens med beskrivningen av *begränsning*, dvs. att den personuppgiftsansvarige vidtar en åtgärd med personuppgifterna som visar att behandlingen har begränsats. Hur begränsningen bör göras får bedömas med utgångspunkt i vad som är lämpligt i det enskilda fallet. En naturlig åtgärd kan vara att avskilja uppgifterna från det datasystem där de behandlas. Begränsningen kan också ha formen av en teknisk begränsning. En tredje möjlighet att begränsa behandlingen är att inskränka tillgången till uppgifterna.

Biometriska uppgifter

Utredningen föreslår att en definition av begreppet Biometriska uppgifter bör införas i de nya lagarna och definieras som ”Personuppgifter som rör en persons fysiska, fysiologiska eller beteendemässiga kännetecken, som tagits fram genom särskild teknisk behandling och som möjliggör eller bekräftar unik identifiering av personen i fråga.”

Begreppet har inte definierats i FM-PuL och FRA-PuL. Den föreslagna definitionen stämmer överens med förslaget till Säkerhetspolisens datalag och i huvudsak med dataskyddsförordningen. Biometriska uppgifter behandlas under avsnitt 6.4.2.

Dataskyddsombud

Personuppgiftsombud definieras i FM-PuL och FRA-PuL som den fysiska person som, efter förordnande av den personuppgiftsansvarige, självständigt ska se till att personuppgifter behandlas på ett korrekt och lagligt sätt.

Funktionen som enligt nuvarande lag benämns personuppgiftsombud föreslås fortsättningsvis benämnas dataskyddsombud och definieras som en fysisk person som utses av den personuppgiftsansvarige för att självständigt se till att personuppgifter behandlas författningsenligt och på ett korrekt sätt.

Motiven för ändringen utvecklas under avsnitt 6.6.5.

Genetiska uppgifter

Utredningen föreslår att en definition av begreppet Genetiska uppgifter bör införas i de nya lagarna och definieras som ”Personuppgifter som rör en persons nedärvda eller förvärvade genetiska kännetecken och som härrör från analys av ett spår av eller ett prov från personen i fråga”.

Begreppet har inte definierats i FM-PuL och FRA-PuL. Den föreslagna definitionen stämmer överens med förslaget till lagen om behandling av personuppgifter vid Säkerhetspolisen och i huvudsak med dataskyddsförordningen. Genetiska uppgifter behandlas under avsnitt 6.4.2.

Logg

Logg definieras inte i FM-PuL och FRA-PuL. Utredningen föreslår att en logg definieras som en behandlingshistorik som sparas viss tid.

Loggning och logguppföljning behandlas under avsnitt 6.6.2.

Mottagare

Mottagare definieras i FM-PuL och FRA-PuL som den till vilken personuppgifter lämnas ut. När personuppgifter lämnas ut från Försvarsmakten eller Försvarets radioanstalt för att en annan myndighet ska kunna utföra sådan tillsyn, kontroll eller revision som den är skyldig att sköta, anses dock inte den myndigheten som mottagare.

Mottagare definieras på samma sätt, något annorlunda uttryckt, i brottsdatalagen och förslaget till Säkerhetspolisens datalag (SOU 2017:74 s. 36) som ”den till vilken personuppgifter lämnas ut, med undantag av en myndighet som med stöd av författning utövar tillsyn, kontroll eller revision.”

Utredningen föreslår att mottagare i de nya lagarna ska definieras på samma sätt som i förslaget till Säkerhetspolisens datalag. Ändringen i förhållande till FM-PuL och FRA-PuL är endast av språklig karaktär.

Personuppgift

Personuppgifter definieras i FM-PuL och FRA-PuL som all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet.

Utredningen föreslår att personuppgifter i de nya lagarna definieras som ”Varje upplysning om en identifierad eller identifierbar fysisk person som är i livet”, i likhet med bl.a. dataskyddsförordningen. Den nya lydelsen innebär inte någon ändring i sak, men gör definitionen enhetlig med övriga lagar på personuppgiftsområdet.

Personuppgiftsansvarig

Utredningen föreslår att en definition av begreppet Personuppgiftsansvarig införs i de nya lagarna och definieras som ”Den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter”.

Begreppet har inte definierats i FM-PuL och FRA-PuL. Den föreslagna definitionen stämmer överens med förslaget till Säkerhetspolisens datalag.

Personuppgiftsbiträde

Utredningen föreslår att definitionen av begreppet Personuppgiftsbiträde ska definieras i de nya lagarna som ”den som, med stöd av ett skriftligt avtal eller annan skriftlig överenskommelse, behandlar personuppgifter för den personuppgiftsansvariges räkning”.

Den föreslagna definitionen, som stämmer överens med förslaget till Säkerhetspolisens datalag, innehåller även ett uttryckligt krav på skriftligt avtal, vilket saknas i definitionen i FM-PuL och FRA-PuL (krav på skriftligt avtal framgår emellertid av 3 kap. 1 § FM-PuL och FRA-PuL). Den föreslagna lydelsen avviker från dataskyddsförordningens definition som inte innehåller krav på skriftligt avtal.

Tredje part

Tredje man definieras i FM-PuL och FRA-PuL som någon annan än den registrerade, den personuppgiftsansvarige, personuppgiftsombudet, personuppgiftsbiträdet och sådana personer som under den personuppgiftsansvariges eller personuppgiftsbiträdets direkta ansvar har befogenhet att behandla personuppgifter.

Utredningen föreslår att termen ska ändras till tredje part med oförändrad lydelse i övrigt. Skälen för förslaget är att det saknas skäl att hålla fast vid *man* i detta sammanhang när betydelsen är helt frikopplad från ordets egentliga betydelse. Även dataskyddsförordningen, som flertalet övriga svenska myndigheter, företag och organisationer kommer att tillämpa, anger numera *tredje part*. Inte heller *man* i betydelsen människa utgör skäl att behålla man i nu aktuella lagar eftersom en utomstående i sammanhanget likaväl kan

vara en myndighet, sammanslutning eller organisation. Förslaget avviker i denna del från förslaget till Säkerhetspolisens datalag.

Uppgiftssamling

Uppgiftssamling definieras i FM-PuL och FRA-PuL som en samling med uppgifter som med hjälp av automatiserad behandling används gemensamt.

Utredningen föreslår att definitionen ska införas i de nya lagarna med den ändringen att används gemensamt" byts ut mot "är gemensamt tillgängliga".

Begreppets innebörd behandlas i avsnitt 6.5.1.

6.3 Behandlingen av personuppgifter

6.3.1 Försvar och säkerhet som rättslig grund för behandling av personuppgifter hos Försvarsmakten

Utredningens förslag: Försvarsmakten får behandla personuppgifter om det är nödvändigt för att planera, förbereda och genomföra verksamhet som rör

1. Sveriges försvar och säkerhet, eller
2. internationellt försvars- och säkerhetssamarbete.

Försvarsmaktens uppgift att bedriva sådan verksamhet ska framgå av lag, förordning eller ett särskilt beslut i vilket regeringen uppdragit åt myndigheten att ansvara för uppgiften.

Skäl för utredningens förslag: Personuppgifter får enligt den föreslagna bestämmelsen behandlas i Försvarsmaktens verksamhet om behandlingen är nödvändig för att planera, förbereda och genomföra verksamhet som rör Sveriges försvar och säkerhet. Försvarsmaktens uppgift att bedriva sådan verksamhet ska framgå av lag, förordning eller ett särskilt beslut i vilket regeringen uppdragit åt myndigheten att ansvara för uppgiften.

Regler om denna verksamhet omfattas inte av unionsrätten och enligt utredningens mening bör någon ändring härvidlag inte göras utan här bör enbart nationella bestämmelser gälla.

I det följande beskriver utredningen vilken verksamhet i Försvarsmakten som den föreslagna bestämmelsen omfattar. Till en del innebär beskrivningen en upprepning av bakgrundsbeskrivningen i avsnitt 3.1 men bedöms nödvändig här för att ge en uppfattning om den personuppgiftsbehandling som är aktuell i sammanhanget.

Som framgår av avsnitt 3.1 har Försvarsmakten i uppdrag att upprätthålla och utveckla ett militärt försvar som ytterst kan möta ett väpnat angrepp samt att försvara Sverige och främja svensk säkerhet. Grunden för Försvarsmaktens verksamhet är förmågan till väpnad strid.

Vid höjd beredskap ska Försvarsmakten kunna krigsorganisera, mobilisera och använda alla krigsförband för att möta ett militärt hot mot Sverige och svenska intressen. Krigsförband ska kunna krigsorganiseras, även om höjd beredskap inte råder. Krigsorganisationen och planeringen av denna innefattar personuppgiftsbehandling av anställda i Försvarsmakten och andra som på annat sätt är knutna till myndigheten.

Behandlingen avser:

1. yrkesofficerare, kontinuerligt tjänstgörande anställda gruppbefäl, soldater och sjömän och Försvarsmaktens civila arbetstagare,
2. de som är tidsbegränsat anställda med stöd av 2 § lagen (2010:449) om Försvarsmaktens personal vid internationella militära insatser,
3. officersaspiranter,
4. reservofficerare och tidvis tjänstgörande anställda gruppbefäl, soldater och sjömän,
5. hemvärnsmän och frivillig personal,
6. den som är inskriven för värnplikt och som tjänstgör i Försvarsmakten, och
7. krigsfrivilliga.

När det gäller personal i krigsorganisationen som inte är anställd i Försvarsmakten bör personuppgiftsbehandlingen enbart gälla uppgifterna i krigsorganisationen. Detta blir en följd av kravet att personuppgiftsbehandlingen ska vara nödvändig för att upprätta och utveckla ett militärt försvar eller för att försvara Sverige. Det är bara i dessa sammanhang som det kravet gör sig gällande för denna personalkategori.

För de anställda i Försvarsmakten tillkommer emellertid att de också är föremål för Försvarsmaktens personuppgiftsbehandling i den för alla myndigheter normala personaladministrativa verksamheten, såsom hanteringen av löner, ledigheter etc. Den personuppgiftsbehandlingen har dock ett nära samband med den som avser krigsorganisationen och planeringen av denna. Det är enligt utredningens mening inte lämpligt att de separeras på så sätt att de kommer att omfattas av skilda regelsystem. För att på ett ändamålsenligt sätt upprätthålla och utveckla Sveriges militära försvar eller för att försvara Sverige är det enligt utredningens mening nödvändigt att de omfattas av samma reglering.

När det gäller Försvarsmaktens krigsorganisation omfattar bestämmelsen således behandlingen av personuppgifter som rör anställda i Försvarsmakten och annan personal som ingår i eller kan komma att ingå i myndighetens krigsorganisation.

Operationer och övningar är nödvändiga för Försvarsmaktens uppdrag att upprätthålla och utveckla ett militärt försvar och att ha förmåga till väpnad strid. När Försvarsmakten planerar, förbereder och genomför militära operationer och övningar behandlar myndigheten uppgifter om de som deltar i operationerna och övningarna. I dessa kan andra än personal i krigsorganisationen delta. Vid genomförande av nationella militära operationer och internationella militära insatser behandlar Försvarsmakten även uppgifter om motståndare eller andra aktörer. Även denna personuppgiftsbehandling omfattas av bestämmelsen.

Enligt förordningen (1982:765) om Försvarsmaktens ingripanden vid kränkningar av Sveriges territorium under fred och neutralitet m.m. (IKFN) ska Försvarsmakten bl.a. upptäcka och avvisa kränkningar av svenskt territorium och i samarbete med civila myndigheter ingripa vid andra överträdelser av tillträdesförordningen (1992:118). Vid dessa ingripanden kan personuppgifter komma att behandlas. Sådan behandling omfattas också av bestämmelsen.

En annan verksamhet när det gäller att upprätthålla och utveckla ett militärt försvar är utveckling av teknik och metodik (se vidare avsnitt 3.1). Det är oundvikligt att verksamhet som bl.a. syftar till att pröva och anpassa teknisk utrustning och tekniska system leder till att personuppgifter behandlas. Även i detta sammanhang kan det bli aktuellt med behandling av personuppgifter. Också sådan behandling omfattas av bestämmelsen.

Som anges i avsnitt 3.1. bedriver Försvarsmakten till stöd för lösandet av Försvarsmaktens militära uppgifter underrättelseverksamhet som inte utgör försvarsunderrättelseverksamhet eller militär säkerhetstjänst. Personuppgiftsbehandlingen inom denna underrättelseverksamhet rör Sveriges försvar och säkerhet och omfattas därför av bestämmelsen.

Försvarsmakten har vidare vissa andra arbetsuppgifter som rör Sveriges försvar och säkerhet och som anges i lag eller förordning. I avsnitt 3.1 ges ett antal exempel på sådana uppgifter. De gäller stöd till polisen vid terrorismbekämpning, omvärldsbevakning och viss attachéverksamhet. Där anges också utnyttjande av personal inom Kustbevakningen, polismäns deltagande i försvaret av riket i krig samt utredningar för att bedöma totalförsvarspliktigas förutsättningar att fullgöra värnplikt.

Den personuppgiftsbehandling som är nödvändig för Försvarsmakten att genomföra de nu nämnda verksamheterna omfattas av bestämmelsen. Beskrivningen av verksamheterna gör inte anspråk på att vara fullständig. Det kan finnas andra uppgifter för Försvarsmakten som rör Sveriges försvar och säkerhet. Sådana kan också tillkomma.

Avslutningsvis vill utredningen nämna några författningsenliga uppgifter som klart faller utanför bestämmelsen. Som tidigare antytts ska myndigheten enligt 2 § andra stycket förordningen (2007:1266) med instruktion för Försvarsmakten med myndighetens befintliga förmåga och resurser kunna lämna stöd till civil verksamhet, se vidare härom förordningen (2002:375) om Försvarsmaktens stöd till civil verksamhet. Enligt 3 § förordningen med instruktion för Försvarsmakten ska myndigheten ansvara för att samla in, bearbeta och lämna Kustbevakningen sjölägesinformation sammanställd för civila behov och på begäran av polisen utföra helikoptertransporter som är av större vikt för genomförandet av polisiära insatser, se härom vidare förordningen (2017:113) om Försvarsmaktens stöd till polisen med helikoptertransporter. Slutligen ska nämnas förordningen (2000:278) om gåvor och överföringar av överskottsmateriel hos Försvarsmakten.

Den föreslagna bestämmelsen omfattar i och för sig också Försvarsmaktens försvarsunderrättelsetjänst och militära säkerhetstjänst. Med hänsyn till dessa verksamheters karaktär och till att de hittills har reglerats i FM-PuL anser utredningen att de även i den föreslagna lagen ska regleras särskilt.

Internationellt försvars- och säkerhetssamarbete

Personuppgifter får enligt den föreslagna bestämmelsen behandlas i Försvarsmaktens verksamhet om behandlingen är nödvändig för att planera, förbereda och genomföra verksamhet som avser internationellt försvars- och säkerhetssamarbete. Försvarsmaktens uppgift att bedriva sådan verksamhet ska framgå av lag, förordning eller ett särskilt beslut i vilket regeringen uppdragit åt myndigheten att ansvara för uppgiften. I 2 § och 3 a § förordningen med instruktion för Försvarsmakten ges Försvarsmakten uppdrag av detta slag. En närmare beskrivning av Försvarsmaktens internationella samarbeten finns i avsnitt 3.1. Här ska endast konstateras att det inom dessa samarbeten behandlas uppgifter som kan avse andra personer än de som ingår eller kan komma att ingå i krigsorganisationen. Sådan behandling omfattas av bestämmelsen.

6.3.2 Försvarsunderrättelseverksamhet som rättslig grund för behandling av personuppgifter hos Försvarsmakten

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

De personuppgifter som Försvarsmakten har fått tillgång i myndighetens försvarsunderrättelseverksamhet får fortsatt behandlas i den verksamheten, om det behövs för att fullfölja den.

Detta gäller dock endast om inget annat följer av den föreslagna lagen om behandling av personuppgifter hos Försvarsmakten eller förordning som regeringen har meddelat i anslutning till den lagen.

Skäl för utredningens förslag: Av 1 kap. 8 § första stycket FM-PuL framgår att personuppgifter får behandlas i Försvarsmaktens försvarsunderrättelseverksamhet om det är nödvändigt för att bedriva den verksamhet som anges i lagen (2000:130) om försvarsunderrättelseverksamhet. Enligt nämnda lag ska försvarsunderrättelseverksamhet bedrivas till stöd för svensk utrikes-, säkerhets- och försvarspolitik samt i övrigt för kartläggning av yttre hot mot landet. Det anges vidare att i verksamheten ingår att medverka i svenskt deltagande i internationellt säkerhetssamarbete och att försvarsunderrättelseverksamheten endast får avse utländska förhållanden. Enligt lagen ska regeringen bestämma försvarsunderrättelseverksamhetens inriktning och inom ramen för denna inriktning får de myndigheter som regeringen bestämmer ange en närmare inriktning av verksamheten. Regeringen brukar bestämma detta i ett årligt inriktningsbeslut. Verksamheten ska fullgöras genom inhämtning, bearbetning och analys av information. Underrättelser ska rapporteras till berörda myndigheter.

Försvarsmakten beslutar för varje år en inhämtandeplan som bl.a. utgör en prioritering av vad myndigheten anser sig kunna utföra av de behov som uppdragsgivarna genom sina inriktningar har angett. I FM-PuL kommer detta till uttryck indirekt genom föreskriften i 1 kap. 8 § andra stycket om preciserad inriktning, som berörs närmare i det följande. I planen kan myndigheten göra de prioriteringar som den anser vara nödvändiga för att avgränsa verksamheten. Planen är också viktig för att uppfylla kravet att personuppgifter får behandlas bara för särskilda, uttryckligt angivna och berättigade ändamål. Utredningen återkommer till detta i avsnitt 6.4.

Regeringens inriktning och de närmare inriktningarna anger behoven av underrättelser, dvs. *vilken* information som efterfrågas. *Hur* detta ska uppnås avgörs av den som utför uppgiften. För Försvarsmaktens del är inhämtandeplanen ett instrument för detta. Som Wilhelm Agrell anför i boken Konsten att gissa rätt är underrättelsebehoven i sig ingen styrfunktion utan det är först när behoven omsätts i planering som de kan resultera i det konkreta arbete som underrättelseprocessen förutsätter.[1]

[1] Agrell, Wilhelm, Konsten att gissa rätt, underrättelsevetenskapens grunder, Studentlitteratur, Lund 1998.

Som regeringen anför i den proposition som ligger till grund för nuvarande reglering av behandlingen av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet är ändamålet för behandlingen att myndigheten ska kunna fullfölja de uppgifter som åligger myndigheten enligt lagen om försvarsunderrättelseverksamhet och den därtill hörande förordningen (prop. 2006/07:46 s. 64). Regeringen förklarade att det inte är möjligt att i lagtext närmare precisera de ändamål för vilka personuppgifter får behandlas i försvarsunderrättelseverksamheten (se a. prop. s. 65). Det kan här tilläggas att det i den senare tillkomna lagen om signalspaning i försvarsunderrättelseverksamhet anges åtta olika syften för signalspaningen (1 § andra stycket).

Enligt 1 kap. 8 § andra stycket FM-PuL får uppgifter om en person endast behandlas om personen har anknytning till en preciserad inriktning för försvarsunderrättelseverksamheten och behandlingen är nödvändig för att fullfölja den inriktningen. Vad som menas med preciserad inriktning anges inte i lagen utan har i praxis ansetts vara den nyss nämnda inhämtandeplanen.

I tillämpningen har fråga uppkommit om bestämmelsen om anknytning till preciserad inriktning innebär att varje personuppgift som behandlas i försvarsunderrättelseverksamheten måste hänföras direkt till regeringens vid varje tidpunkt gällande inriktning. Ett annat synsätt är att uppfattningen om anknytningens betydelse i sammanhanget inte bör drivas så långt. I stället räcker det att den indirekt berörs av den preciserade inriktningen på så sätt att behandlingen av personuppgiften behövs för att fullfölja det som följer av regeringens och andra uppdragsgivares inriktning. Den osäkerhet som kan finnas när det gäller innebörden av anknytningen till preciserad inriktning befrämjar enligt utredningens mening inte en effektiv underrättelseverksamhet. Utredningen anser därtill att kravet på anknytning till en preciserad inriktning kan ifrågasättas. Inriktningarna och planeringen utgör avgränsningar av behandlingen av personuppgifter på så sätt att de anger underrättelsebehoven. Men med ledning av inriktningarna och planeringen kan man inte i detalj avgöra vilken personuppgiftsbehandling som kan vara och bli nödvändig.

I underrättelseverksamhetens natur ligger nämligen att det inte går att på förhand göra tydliga avgränsningar av vilka uppgifter som måste inhämtas för att nå det slutliga målet att åstadkomma de

underrättelser som uppdragsgivarna efterfrågar. Inhämtad information kan motivera inhämtning av annan information som man från början inte kände till. Det kan också uppkomma behov av att värdera trovärdigheten hos källor, som man heller inte kände till från början. Särskilt tydligt blir det nu sagda när verksamheten till stora delar går ut på att leta efter företeelser och hot som är okända men som man antar existerar.

I sammanhanget vill utredningen också peka på följande förhållanden. Försvarsunderrättelseverksamhet är huvudsakligen framåtsyftande. Den kartlägger företeelser i syfte att kunna förvarna om bl.a. avsikter, aktiviteter och hot till stöd för de inriktande myndigheternas egna verksamheter. Kartläggningar avser bl.a. skeenden, organisationer och aktörer av betydelse för förståelsen för den omvärldsutveckling som inriktningarna adresserar. För att kunna förstå ett skeende eller en aktörs agerande behöver det observerade emellertid ofta sättas in i ett kontextuellt och historiskt sammanhang. Först därefter kan bedömningar om det observerades underrättelserelevans göras. Det som observeras i dag behöver således jämföras med tidigare observationer. För vissa företeelser behöver sådana jämförelser kunna göras med observationer som gjordes långt tillbaka i tiden, inte sällan 10–20 år tillbaka. Vedertagna begrepp i sammanhanget är normalbild respektive avvikelse från normalbild. Av detta följer att underrättelseverksamhet alltid måste behandla äldre information, inklusive personuppgifter, för att man ska kunna förstå och bedöma den underrättelsemässiga relevansen av sådant som sker i dag.

Det som nu har sagts visar enligt utredningens mening att underrättelseverksamhet som bedrivs enligt lagen om försvarsunderrättelseverksamhet måste kunna avse förhållanden som inte alltid direkt kan hänföras till regeringens vid varje tidpunkt gällande inriktning så länge dessa förhållanden har betydelse för fullföljandet av det uppdrag som inriktningen innebär. Därmed måste det också vara möjligt att behandla personuppgifter som rör dessa förhållanden. Detta kommer till uttryck i den föreslagna regleringen på så sätt att personuppgifter får behandlas i Försvarsmaktens försvarsunderrättelseverksamhet om det är nödvändigt för att bedriva den verksamhet som anges i lagen om försvarsunderrättelseverksamhet. Enligt utredningen får detta anses vara en tillräcklig ändamålsbeskrivning som dock i förtydligande syfte bör kompletteras i två avseenden till

vilka utredningen återkommer i det följande och avsnitt 6.3.4. Utredningen anser således att den nuvarande ordningen med kravet på anknytning till en preciserad inriktning inte bör behållas.

Genom den föreslagna regleringen av ändamålen med personuppgiftsbehandlingen i försvarsunderrättelseverksamheten kommer, som utredningen nyss nämnde, behandlingen kunna avse förhållanden som inte alltid direkt kan hänföras till regeringens vid varje tidpunkt gällande inriktning så länge dessa förhållanden har betydelse för fullföljandet av det försvarsunderrättelseuppdrag som följer av inriktningen.

Som ovan anförts måste en underrättelseverksamhet behandla äldre information, inklusive personuppgifter, för att man ska kunna förstå och bedöma den underrättelsemässiga relevansen av sådant som sker i dag. För tydlighetens skull anser utredningen att ändamålsbeskrivningen bör kompletteras med en föreskrift som innebär att de personuppgifter som Försvarsmakten har fått tillgång till i sin försvarsunderrättelseverksamhet fortsatt får behandlas i den verksamheten, om det behövs för att fullgöra den.

Detta bör dock endast gälla om inget annat följer av den föreslagna lagen om behandling av personuppgifter vid Försvarsmakten eller förordning som regeringen har meddelat i anslutning till den lagen.

Den föreslagna föreskriften ger också ett stöd för behandling av uppgifter som behövs för att Försvarsmakten ska kunna uppfylla de krav som uppdragsgivarna ställer på snabbhet och flexibilitet i samband med internationella kriser och andra hastigt uppkomna händelser.

6.3.3 Militär säkerhetstjänst som rättslig grund för behandling av personuppgifter hos Försvarsmakten

Utredningens förslag: Personuppgifter får behandlas i Försvarsmaktens militära säkerhetstjänst för att upptäcka, förebygga och avvärja säkerhetshotande verksamhet som riktas mot Försvarsmakten och dess säkerhetsintressen, om det är nödvändigt för att

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

Uppgifter om en person får behandlas för de angivna ändamålen endast om

1. uppgifterna är nödvändiga för att kartlägga verksamhet som innefattar brott som kan hota Sveriges säkerhet eller terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott eller motsvarande brottslighet enligt tidigare lagstiftning,
2. uppgifterna är nödvändiga för att kartlägga underrättelseverksamhet riktad mot Försvarsmakten och dess säkerhetsintressen,
3. uppgifterna är nödvändiga för att kartlägga annan säkerhetshotande verksamhet än som avses i 1 och som innefattar brott eller åsidosättande av åligganden i anställning hos Försvarsmakten, och det finns särskilda skäl till att uppgiften ska behandlas,
4. personen har lämnat uppgifter om säkerhetshotande verksamhet och personuppgifterna är nödvändiga för att bedöma personens trovärdighet,
5. uppgifterna avser information som har framkommit i samband med säkerhetsprövning enligt säkerhetsskyddslagen (1996:627) eller i annat fall är nödvändiga för att utföra en uppgift som rör säkerhetsskydd.

Personuppgifter som behandlas enligt ovan ska förses med upplysning om på vilken av de angivna grunderna uppgiften behandlas.

Om behandlingen av en personuppgift föranleds av något annat än antagande om att personen har utövat eller kommer att utöva brottslig verksamhet ska 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 ska förses med en särskild upplysning om detta, om det inte på annat sätt klart framgår att sådant antagande inte finns.

Personuppgifter som behandlas enligt punkterna 1–3 ska i förekommande fall förses med en upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak.

Trots vad som sägs ovan får personuppgifter som ingår i eller har uppkommit i samband med användning av totalförsvarets telekommunikations- och informationssystem behandlas för att förhindra obehörig insyn i och påverkan av dessa system. Det gäller även känsliga personuppgifter och personuppgifter där den som uppgifterna rör har offentliggjort dem eller lämnat sitt samtyckes. Behandling som särskilt syftar till att identifiera en person får dock endast utföras om bestämmelserna i punkterna 1, 2 eller 3 tillämpas.

Skäl för utredningens förslag: Liksom konstaterats beträffande försvarsunderrättelseverksamheten definieras inte heller vad som avses med militär säkerhetstjänst i FM-PuL. Ledning får därför hämtas i säkerhetsskyddslagen (1996:627) och säkerhetsskyddsförordningen (1996:633). Ändamålet med behandlingen av personuppgifter inom den militära säkerhetstjänsten är att tjänsten ska kunna fullgöra de uppgifter som följer av säkerhetsskyddslagen, den därtill hörande förordningen och förordningen med instruktion för Försvarsmakten. Regeringen föreslog därför i motiven till de nuvarande bestämmelserna, att personuppgifter ska få behandlas i den militära säkerhetstjänstens verksamhet med att upptäcka, förebygga och avvärja säkerhetshotande verksamhet som riktas mot Försvarsmakten och dess säkerhetsintressen, om det är nödvändigt för att klarlägga verksamhet som innefattar hot mot rikets säkerhet. Denna säkerhetsverksamhet kallas säkerhetsunderrättelsetjänst. I samma syfte ska personuppgifter få behandlas, om det är nödvändigt för att vidta åtgärder som hindrar eller

försvårar säkerhetshotande verksamhet. Då är det fråga om säkerhetsskyddstjänst. Även inom signalskyddstjänsten, som är en säkerhetsskyddsangelägenhet, kan arbete förekomma som avser att klarlägga säkerhetshotande verksamhet. Signalskyddstjänsten innefattar, liksom säkerhetsskyddstjänsten, åtgärder för att hindra eller försvåra säkerhetshotande verksamhet, varför den inte behöver regleras särskilt. I motiven till den nuvarande regleringen angavs även att det saknas behov av att i lagen ange de olika verksamhetsgrenarna inom den militära säkerhetstjänsten (prop. 2006/07:46 s. 65 f.).

Den militära säkerhetstjänsten är en grundläggande verksamhet för Sveriges försvar och nationell säkerhet omfattas därmed inte av unionsrätten. Enligt utredningens mening bör personuppgiftsbehandlingen såvitt avser denna verksamhet även fortsatt regleras särskilt och omfattas av den föreslagna särlagstiftningen.

Som framgår av avsnitt 5.1.2 får personuppgifter behandlas i Försvarsmaktens militära säkerhetstjänst för att upptäcka, förebygga och avvärja säkerhetshotande verksamhet som riktas mot Försvarsmakten och dess säkerhetsintressen, om det är nödvändigt för att klarlägga verksamhet som innefattar hot mot rikets säkerhet, eller vidta åtgärder som hindrar eller försvårar säkerhetshotande verksamhet (1 kap. 9 § FM-PuL). Utredningen anser att den bestämmelsen bör föras in i den nya lagen.

Utredningen föreslår att de närmare bestämmelserna som anger villkoren för personuppgiftsbehandlingen utformas på samma sätt i den nya lagen som i den nuvarande med de ändringar som framgår av det följande.

Enligt *första* och *andra punkterna* får uppgifter behandlas för att kartlägga verksamhet som innefattar brott som kan hota rikets säkerhet eller terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott eller motsvarande brottslighet enligt tidigare lagstiftning eller om uppgifterna är nödvändiga för att kartlägga underrättelseverksamhet riktad mot Försvarsmakten och dess säkerhetsintressen. Genom uttrycket ”kartlägga” blir bestämmelserna även tillämpliga på uppgifter om sådana personer som kan betraktas som sekundära i förhållande till den som utgör hotet eller utövar underrättelseverksamheten men som ändå är av betydelse för att klarlägga verksamhet som innefattar hot mot Sveriges säkerhet.

Enligt *tredje punkten* får uppgifter behandlas för de angivna ändamålen om uppgifterna är nödvändiga för att kartlägga annan säkerhetshotande verksamhet och som innefattar brott eller åsidosättande av åligganden i anställning hos Försvarsmakten, och det finns särskilda skäl till att uppgifterna behandlas. Även här blir det möjligt att behandla uppgifter om sådana personer som kan betraktas som sekundära i förhållande till den som utövar den säkerhetshotande verksamheten men som ändå är av betydelse för att klarlägga denna verksamhet.

Kravet på särskilda skäl innebär att personuppgifter inte får behandlas vid en rent bagatellartad förseelse som inte ens om den upprepades eller sammantaget med annan verksamhet skulle föranleda någon åtgärd. Någon ytterligare omständighet erfordras för att behandling ska få ske, t.ex. att det bedöms föreligga risk för upprepning eller att personen i fråga har en sådan position att uppföljning är nödvändig. Som en grundläggande förutsättning gäller att den säkerhetshotande verksamheten ska vara riktad mot Försvarsmakten och dess säkerhetsintressen (prop. 2006/07:46 s. 70 f.).

Enligt *fjärde* och *femte punkterna* får uppgifter behandlas för de angivna ändamålen om personen har lämnat uppgifter om säkerhetshotande verksamhet och personuppgifterna är nödvändiga för att bedöma personens trovärdighet (fjärde punkten) eller om uppgifterna har framkommit genom att någon genomgått en säkerhetsprövning enligt säkerhetsskyddslagen (femte punkten).

Beträffande femte punkten gör utredningen följande överväganden i fråga om uttrycket ”säkerhetsprövning”. Försvarsmakten ska leda och bedriva militär säkerhetstjänst och måste för att uppfylla syftet med säkerhetsskyddslagen vidta vissa säkerhetsskyddsåtgärder. Dessa åtgärder benämns i säkerhetsskyddslagen informationssäkerhet, tillträdesbegränsning samt säkerhetsprövning. I bestämmelsen i femte punkten behöver således ”säkerhetsprövning” ersätta tidigare uttrycken ”registerkontroll eller särskild personutredning”. Skälet är att säkerhetsprövning är ett vidare begrepp som innefattar mer än registerkontroll eller särskild personutredning. Av 14 § säkerhetsskyddsförordningen framgår nämligen att säkerhetsprövningen grundas på

1. den personliga kännedom som finns om den som prövningen gäller,
2. uppgifter som framgår av betyg, intyg och referenser, samt om bestämmelserna om sådana åtgärder är tillämpliga
3. uppgifter som har kommit fram vid registerkontroll och särskild personutredning.

Femte punkten bör således täcka in alla delar i en säkerhetsprövning enligt säkerhetsskyddslagen, vilket bör framgå direkt av författningstexten.[2]

Av femte punkten bör även framgå att uppgifter om en person får behandlas för de angivna ändamålen om de i annat fall är nödvändiga för att utföra en uppgift som rör säkerhetsskydd. Exempel på sådana uppgifter är Försvarsmaktens tillträdeskontroll vid objekt, lokaler och områden där Försvarsmakten bedriver verksamhet som kräver säkerhetsskydd, behörighetshantering inom signalskyddstjänsten, utbildning i säkerhetsskydd och kontroll av säkerhetsloggar.

Enligt 1 kap. 10 § andra stycket FM-PuL ska uppgifter om en person som behandlas inom den militära säkerhetstjänsten förses med upplysning om på vilken av de angivna grunderna uppgiften behandlas. Om behandlingen av en personuppgift föranleds av något annat än antagande om att personen har utövat eller kommer att utöva brottslig verksamhet ska 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 ska förses med en särskild upplysning om detta, om det inte på annat sätt klart framgår att sådant antagande inte finns.

Av 1 kap. 10 § tredje stycket FM-PuL framgår att uppgifter som om en person ska förses med en upplysning om på vilken av grund uppgiften behandlas. Uppgifter om en person som lämnat uppgifter om säkerhetshotande verksamhet ska förses med en upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak.

[2] Se även prop. 1995/96:129 om säkerhetsskydd (s. 78) samt prop. 2006/07:46 s. 67, där det beskrivs att personuppgifter behandlas när någon varit föremål för säkerhetsprövning enligt säkerhetsskyddslagen.

Motiven till bestämmelserna finns i prop. 2006/07:46 s. 70 f. och 122.

Utredningen föreslår att bestämmelser som motsvarar 1 kap. 10 § andra och tredje styckena FM-PuL införs i den nya lagen.

Enligt 1 kap. 11 § FM-PuL får, trots vad som krävs avseende rättslig grund för behandlingen enligt bestämmelserna ovan, personuppgifter som ingår i eller har uppkommit i samband med användning av totalförsvarets telekommunikations- och informationssystem behandlas 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 någon av grunderna i punkterna 1, 2 eller 3 tillämpas. Enligt andra stycket samma bestämmelse ska Försvarsmakten föra en förteckning över de behandlingar som särskilt syftar till att identifiera en person och de uppgifter som utgjort anledningen till behandlingen.

Motiven till bestämmelsen finns i prop. 2006/07:46 s. 72 f. och 123).

Utredningen föreslår att en motsvarande bestämmelse införs i den nya lagen.

I 1 kap. 11 § andra stycket FM-PuL finns en bestämmelse om att Försvarsmakten ska föra en förteckning över sådana behandlingar, av vilken ska framgå vilken person som avsetts med behandlingen och de uppgifter som utgjort anledningen till behandlingen. En sådan förteckning för att möjliggöra kontroll i efterhand av grunden för att en behandling utförts i syfte att identifiera en person. Utredningen föreslår inte någon sådan bestämmelse i den nya lagen eftersom Försvarsmakten är skyldig att spara sådana uppgifter redan på grund av bestämmelserna om krav på rättslig grund, loggning m.m. Vidare har dataskyddsombudet till uppgift att föra förteckning över behandlingar.

6.3.4 Rättsliga grunder för behandling vid Försvarsmakten av personuppgifter som utgör allmänt tillgänglig information

Utredningens förslag: Personuppgifter som utgör allmänt tillgänglig information får behandlas av Försvarsmakten om det är nödvändigt för

1. planering, förberedelse och genomförande av verksamhet som rör Sveriges försvar och säkerhet eller internationellt försvars- och säkerhetssamarbete,
2. försvarsunderrättelseverksamheten, eller
3. den militära säkerhetstjänsten.

Skäl för utredningens förslag: Som tidigare nämnts behöver Försvarsmakten för att kunna bedriva en effektiv försvarsunderrättelseverksamhet utöver den information som den inhämtar genom hemliga metoder, också god tillgång till allmänt tillgänglig information. Därigenom kan den på hemligt sätt inhämtade informationen på ett bättre sätt än eljest sättas in i sitt rätta sammanhang. Av intresse här är information som utgörs av personuppgifter som kan påträffas vid sökning på internet eller vid sökningar i öppna databaser. Uppgifterna kan vara gratis eller tillgängliga på kommersiell grund. Gemensamt för dem är att de är publikt tillgängliga. Det kan röra sig om uppgifter som t.ex. en abonnent på ett eller annat sätt har samtyckt att uppgifterna finns med i elektroniska telefonkataloger eller förteckningar över ip-adresser i olika länder. Eftersom försvarsunderrättelseverksamheten måste vara hemlig är det inte lämpligt att myndigheten exponerar sig eller sina uppdragsgivares underrättelsebehov genom att själv göra sökningar i dessa databaser. I stället måste databaserna anskaffas och läggas upp som referensdatabaser hos myndigheten där den kan göra sökningar.

Ett syfte med att behandla personuppgifter i referensdatabaser kan vara att kunna skaffa ytterligare kunskap om förhållanden av relevans för fullföljandet av en inriktning, t.ex. telefonnummer, adresser, geografisk hemvist etc. Ett annat syfte kan vara att kunna identifiera vem som använder en adressuppgift av intresse, t.ex. telefonnummer som förekommer i den inhämtade informationen.

Det är inte bara i försvarsunderrättelseverksamheten som det finns ett behov av att behandla personuppgifter på det nu beskrivna sättet. Också den militära säkerhetstjänsten har behov av det. Behovet förekommer även när det gäller planering, förberedelse och genomförande av verksamhet som avser Sveriges försvar och säkerhet eller internationellt försvars- och säkerhetssamarbete.

Antalet personuppgifter i myndighetens referensdatabaser kan bli mycket stort. Även om uppgifterna är allmänt tillgängliga innebär ett stort antal en form av integritetsintrång. De föreslagna ändamålsbestämmelserna kan visserligen sägas täcka den nu beskrivna behandlingen av personuppgifter. I klarhetens intresse bör behandlingen dock få ett tydligt stöd i lagen. I lagen bör därför införas en föreskrift om att personuppgifter som utgörs av allmänt tillgänglig information får behandlas av Försvarsmakten om det är nödvändigt för planering, förberedelse och genomförande av verksamhet som avser Sveriges försvar och säkerhet eller internationellt försvars- och säkerhetssamarbete, försvarsunderrättelseverksamheten eller den militära säkerhetstjänsten.

6.3.5 Övriga rättsliga grunder för behandlingen av personuppgifter vid Försvarsmakten

Utredningens förslag: Personuppgifter får även behandlas av Försvarsmakten om det är nödvändigt för diarieföring, arkivering, handläggning av ett ärende eller för att utföra en annan liknande uppgift som åligger myndigheten.

Skäl för utredningens förslag: Försvarsmakten har elektroniska ärendehanteringssystem i vilka personuppgifter är sökbara enligt särskilda kriterier och behörigheter. Diarieföringen vid Försvarsmakten avser handlingar som rör Sveriges försvar och säkerhet. Det samma gäller de arkiverade handlingarna. Ärendehandläggningen vid myndigheten kan avse skadeståndsärenden, tillträdesärenden (ansökan från annan stat om att få tillträde till svenskt territorium), ärenden inom Försvarsmaktens tillsyns- och inspektionsverksamhet, ärenden då Försvarsmakten ansöker om miljötillstånd, ärenden enligt förfogandelagstiftningen, ärenden om kvalificerade skyddsidentiteter och ärenden om utlämnande av allmän handling. Andra uppgifter

som liknar ärendehandläggning och som åligger myndigheten kan vara att besvara frågor rörande Sveriges försvar eller att kommunicera med anställda eller värnpliktiga i frågor som rör deras tjänst. Det kan också gälla utvärdering av den egna verksamheten såsom tidredovisning, lönesättning och sjuktal.

Utredningen anser att den behandling av personuppgifter som uppkommer i de nu beskrivna verksamheterna bör omfattas av den nya lagen.

6.3.6 Försvarsunderrättelseverksamhet som rättslig grund för behandling av personuppgifter vid Försvarets radioanstalt

Utredningens förslag: Personuppgifter får behandlas i Försvarets radioanstalts försvarsunderrättelseverksamhet om det är nödvändigt för att bedriva den verksamhet som anges i lagen (2000:130) om försvarsunderrättelseverksamhet och lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet.

De personuppgifter som Försvarets radioanstalt har fått tillgång till i sin försvarsunderrättelseverksamhet får fortsatt behandlas i den verksamheten, om det behövs för att fullgöra den.

Detta gäller dock endast om inget annat följer av den föreslagna lagen om behandling av personuppgifter vid Försvarets radioanstalt eller förordning som regeringen har meddelat i anslutning till den lagen.

Personuppgifter som behandlas i försvarsunderrättelseverksamheten får även behandlas om det är nödvändigt för att tillhandahålla information som behövs

1. i verksamhet hos berörda myndigheter som avses i 2 § lagen (2000:130) om försvarsunderrättelseverksamhet.
2. med anledning av samarbete med andra länder och internationella organisationer enligt lagen (2000:130) om försvarsunderrättelseverksamhet och lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet.
3. i utvecklingsverksamheten för de ändamål som anges för den verksamheten,

4. i informationssäkerhetsverksamheten för de ändamål som anges för den verksamheten, eller
5. för att biträda andra myndigheter i den utsträckning det följer av lag eller förordning eller om regeringen i ett enskilt fall beslutar om det.

Skäl för utredningens förslag: I FRA-PuL föreskrivs i 1 kap. 8 § första stycket att personuppgifter får behandlas i Försvarets radioanstalts försvarsunderrättelseverksamhet om det är nödvändigt för att bedriva den verksamhet som anges i lagen (2000:130) om försvarsunderrättelseverksamhet. Enligt den lagen ska försvarsunderrättelseverksamhet bedrivas till stöd för svensk utrikes-, säkerhets- och försvarspolitik samt i övrigt för kartläggning av yttre hot mot landet. Det anges vidare att i verksamheten ingår att medverka i svenskt deltagande i internationellt säkerhetssamarbete och att försvarsunderrättelseverksamheten endast får avse utländska förhållanden. I 1 § andra stycket lagen om signalspaning i försvarsunderrättelsetjänst anges att signalspaning får ske endast för att kartlägga

1. yttre militära hot mot landet,
2. förutsättningar för svenskt deltagande i fredsfrämjande och humanitära insatser eller hot mot säkerheten för svenska intressen vid genomförande av sådana insatser,
3. strategiska förhållanden avseende internationell terrorism och annan grov gränsöverskridande brottslighet som kan hota väsentliga nationella intressen
4. utveckling och spridning av massförstörelsevapen, krigsmateriel, och produkter som avses i lagen (200:1064) om kontroll av produkter med dubbla användningsområden och av tekniskt bistånd,
5. allvarliga yttre hot mot samhällets infrastruktur,
6. konflikter utomlands med konsekvenser för internationell säkerhet,
7. främmande underrättelseverksamhet mot svenska intressen, eller
8. främmande makts agerande eller avsikter av väsentlig betydelse för svensk utrikes-, säkerhets- och försvarspolitik.

Enligt lagen om försvarsunderrättelseverksamhet ska regeringen bestämma försvarsunderrättelseverksamhetens inriktning och inom ramen för denna inriktning får de myndigheter som regeringen bestämmer ange en närmare inriktning av verksamheten. Regeringen brukar bestämma detta i inriktningsbeslutet. För Försvarets radioanstalt anges kretsen av uppdragsgivare, såvitt gäller signalspaning, i 4 § första stycket lagen om signalspaning i försvarsunderrättelseverksamhet. Enligt den bestämmelsen får inriktning av signalspaning endast anges av regeringen, Regeringskansliet, Försvarsmakten, Säkerhetspolisen och Nationella operativa avdelningen i Polismyndigheten.

Enligt 1 kap. 8 § andra stycket FRA-PuL får uppgifter om en person endast behandlas om personen har anknytning till en preciserad inriktning för försvarsunderrättelseverksamheten och behandlingen är nödvändig för att fullfölja den inriktningen.

Försvarets radioanstalt beslutar för varje år en preciserad inriktning med produktionsplan som bl.a. utgör en prioritering av vad myndigheten anser sig kunna utföra av de behov som uppdragsgivarna genom sina inriktningar gett uttryck för. I FRA-PuL kommer detta till uttryck indirekt genom föreskriften i 1 kap. 8 § andra stycket om preciserad inriktning, som berörs närmare i det följande. I planen kan myndigheten göra de prioriteringar som den anser vara nödvändiga för att avgränsa verksamheten. Planen är också viktig för att uppfylla kravet att personuppgifter får behandlas bara för särskilda, uttryckligt angivna och berättigade ändamål. Utredningen återkommer till detta i avsnitt 6.4.

Utredningen har i avsnitt 6.3.2 när det gäller Försvarsmaktens försvarsunderrättelseverksamhet kommit fram till att ändamålet för personuppgiftbehandlingen i den verksamheten bör beskrivas så att den ska vara nödvändig för att bedriva försvarsunderrättelseverksamhet. Enligt utredningens mening bör den nuvarande ordningen med krav på anknytning till en preciserad inriktning inte behållas. De skäl och slutsatser som utredningen har fört fram när det gäller ändamålen för personuppgiftsbehandlingen i Försvarsmaktens försvarsunderrättelseverksamhet gäller även personuppgiftsbehandlingen i Försvarets radioanstalts försvarsunderrättelseverksamhet. Ändamålet för personuppgiftsbehandlingen i Försvarets radioanstalts försvarsunderrättelseverksamhet bör således utformas i överensstämmelse med det som utredningen föreslår för personuppgiftsbehandlingen i Försvarsmaktens försvarsunderrättelseverksamhet.

Beskrivningen bör också innehålla en hänvisning till lagen om signalspaning i försvarsunderrättelseverksamhet.

Liksom för Försvarsmaktens del bör ändamålsbeskrivningen kompletteras i två avseenden som utredningen berör i det följande och i avsnitt 6.3.9.

Även Försvarets radioanstalt måste i sin försvarsunderrättelseverksamhet behandla äldre information, inklusive personuppgifter, för att man ska kunna förstå och bedöma den underrättelsemässiga relevansen av sådant som sker i dag. För tydlighetens skull anser utredningen att ändamålsbeskrivningen också för Försvarets radioanstalt bör kompletteras med en föreskrift som innebär att de personuppgifter som myndigheten har fått tillgång till i sin försvarsunderrättelseverksamhet fortsatt får behandlas i den verksamheten, om det behövs för att fullgöra den.

Detta bör dock endast gälla om inget annat följer av den föreslagna lagen om behandling av personuppgifter hos Försvarets radioanstalt eller förordning som regeringen har meddelat i anslutning till den lagen.

På samma sätt som för Försvarsmakten ges härmed ett tydligt stöd för behandling av uppgifter som behövs för att Försvarets radioanstalt ska kunna uppfylla de krav som uppdragsgivarna ställer på snabbhet och flexibilitet i samband med internationella kriser och andra hastigt uppkomna händelser.

Enligt 2 a § lagen om signalspaning i försvarsunderrättelseverksamhet får inhämtning inte avse signaler mellan en avsändare och en mottagare som båda befinner sig i Sverige. Om sådana signaler inte kan avskiljas redan vid inhämtningen, ska upptagningen eller uppteckningen förstöras så snart det står klart att sådana signaler har inhämtats. Om en sådan otillåten inhämtning ändå sker, måste upptagningen eller uppteckningen alltså förstöras. Ett annat fall där en upptagning eller uppteckning ska förstöras regleras i 7 § nämnda lag. Den bestämmelsen tar sikte på vissa i paragrafen angivna uppgifter som inte får behandlas vidare. Förstöringsåtgärderna i båda dessa fall kan innefatta behandling av personuppgifter. Genom att ändamålsbestämmelsen hänvisar till verksamhet som anges i lagen om signalspaning i försvarsunderrättelseverksamhet skapas en rättslig grund för sådan behandling av personuppgifter som är nödvändig för att avskilja personuppgifter som inte ska inhämtas eller behandlas vidare.

Genom signalspaning kan en inhämtad upptagning eller uppteckning innehålla olika personuppgifter. En del är av betydelse för verksamheten medan andra inte är det. Det är ofta inte praktiskt möjligt att separera uppgifter i samma upptagning. Att förstöra hela upptagningen skulle i många fall vara klart menligt för verksamheten och därmed för uppdragsgivarnas behov. Behåller man den innebär det att även de personuppgifter som saknar betydelse kommer att behandlas. Detta är en oundviklig följd om intresset att använda övriga uppgifter i upptagningen är starkt.

Ett liknande resonemang fördes i prop. 2006/07:63 s. 108 och 109 i motiven till bestämmelsen om förstöring i 7 § den där föreslagna lagen om signalspaning i försvarsunderrättelseverksamhet. Där anfördes att det inte går att undvika att inhämtningen kommer att omfatta både relevant och irrelevant information, särskilt inte när inhämtningen förmedlas vid ett och samma kommunikationstillfälle. När det gäller uppgifter om fysiska personer omfattar den då föreslagna bestämmelsen om förstöring av upptagning eller uppteckning bara upptagningar som innehåller betydelselösa uppgifter. Det konstaterades att bestämmelsen inte riktar sig mot upptagningar med både relevant och irrelevant information och att en sådan upptagning ju faktiskt – i vart fall till viss del – har betydelse för verksamheten och då inte ska förstöras. Det bör här nämnas att möjligheten att underlåta förstöring inte gäller de fall som anges i 7 § punkterna 2 och 3 dvs. uppgifter för vilka tystnadsplikt gäller enligt bestämmelser i tryckfrihetsförordningen eller yttrandefrihetsgrundlagen och uppgifter i sådana meddelanden mellan en person som är misstänkt för brott och dennes försvarare som skyddas av vissa bestämmelser i rättegångsbalken. I lagstiftningsärendet konstaterades vidare att problemet med olika typer av uppgifter i en och samma upptagning inte kan lösas genom ett krav på att upptagningen eller uppteckningen ska redigeras så att endast betydelsefull information får kvarstå. En sådan ordning angavs ej vara genomförbar. Problemet fick enligt propositionen lösas genom en bestämmelse om att rapportering av underrättelser som inhämtats genom signalspaning och som innefattar uppgifter som berör fysisk person endast får avse förhållanden som är av betydelse för ändamålet med verksamheten såsom den formuleras i 1 § lagen om försvarsunderrättelseverksamhet.

Utredningen kan konstatera att signalspaningslagstiftningen med det nu beskrivna synsättet kom till efter FRA-PuL Genom att ändamålsbestämmelsen hänvisar till verksamhet som anges i lagen om signalspaning i försvarsunderrättelseverksamhet får det beskrivna förfarandet ett rättsligt stöd.

Vidarebehandling av personuppgifter för vissa andra ändamål än de ursprungliga, får göras med stöd av 1 kap. 6 § 4 p FRA-PuL. Bestämmelsen ger möjlighet att fortsatt behandla insamlade uppgifter så länge personuppgifterna inte behandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in (finalitetsprincipen).

Enligt utredningen mening är det en fördel från integritetsskyddssynpunkt att i görligaste mån precisera i vilka fall personuppgiftsbehandling får ske för andra ändamål än det för vilket uppgifterna har samlats in. I förslaget till Säkerhetspolisens datalag förekommer en sådan reglering.

Till en början vill utredningen peka på två andra verksamheter inom Försvarets radioanstalt. Personuppgifter som behandlas i försvarsunderrättelseverksamheten bör även få behandlas om det är nödvändigt för att tillhandahålla information som behövs i utvecklingsverksamheten för de ändamål som gäller för den verksamheten. Den andra verksamheten är informationssäkerhetsverksamheten. Som framgår av avsnitt 3.3.6 är den nära knuten till vissa delar av försvarsunderrättelseverksamheten vilket ger unika möjligheterna till ökad säkerhet på it-området. Av den anledningen är det viktigt att personuppgifter som behandlas i försvarsunderrättelseverksamheten också får behandlas i informationssäkerhetsverksamheten för de ändamål som anges för den verksamheten.

I ytterligare tre fall är det aktuellt med behandling av personuppgifter för andra ändamål än de ursprungliga. Ett av dem avser verksamhet hos berörda myndigheter enligt 2 § lagen om försvarsunderrättelseverksamhet. Det andra fallet gäller samarbete med andra länder och internationella organisationer enligt lagen om försvarsunderrättelseverksamhet och lagen om signalspaning i försvarsunderrättelseverksamhet. Det tredje fallet avser biträde till andra myndigheter vid anskaffning av signalspaningssystem i den utsträckning det följer av lag eller förordning eller om regeringen i ett enskilt fall beslutar om det. Som nämnts i avsnitt 3.2 har regeringen i instruktionen för Försvarets radioanstalt föreskrivit att radioanstalten ska

biträda andra myndigheter vid värdering, utveckling, anskaffning och drift av signalspaningssystem

Den föreslagna regleringen innebär således att personuppgiftsbehandling för vissa ändamål uttryckligen regleras i lag i stället för att, som tidigare, hanteras i enlighet med finalitetsprincipen. Avsikten är att åstadkomma tydlighet i de nu nämnda fallen. Finalitetsprincipen gäller därutöver.

6.3.7 Utvecklingsverksamhet som rättslig grund för behandling av personuppgifter hos Försvarets radioanstalt

Utredningens förslag: Försvarets radioanstalt får i utvecklingsverksamheten behandla personuppgifter om det är nödvändigt för försvarsunderrättelseverksamheten för att

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

Personuppgifter som behandlas i denna utvecklingsverksamhet får även behandlas om det är nödvändigt för att tillhandahålla information som behövs

1. med anledning av samverkan med annan avseende utvecklingsverksamhet,
2. med anledning av samarbete om utvecklingsverksamhet med utländsk underrättelse- eller säkerhetstjänst enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet,
3. i försvarsunderrättelseverksamheten för de ändamål som anges för den verksamheten.
4. i informationssäkerhetsverksamhet för de ändamål som anges för den verksamheten, eller
5. för att biträda andra myndigheter i den utsträckning det följer av lag eller förordning eller om regeringen i ett enskilt fall beslutar om det.

Skäl för utredningens förslag: Som angetts i avsnitt 3.3.5 ska Försvarets radioanstalt enligt myndighetens instruktion bedriva viss utvecklingsverksamhet och särskilt följa förändringen av signalmiljön i omvärlden, den tekniska utvecklingen och signalskyddet. Myndigheten ska också fortlöpande utveckla den teknik och metodik som behövs för att bedriva verksamheten enligt lagen om signalspaning i försvarsunderrättelseverksamhet. Av 1 § tredje stycket den lagen framgår att signaler i elektronisk form får inhämtas vid signalspaning för dessa syften. Myndigheten ska vidare utföra matematiska bedömningar av kryptosystem för totalförsvaret samt 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 signalspaningsmaterial för att man ska kunna vara säker på teknikens riktighet. Det autentiska materialet kan innehålla personuppgifter. Stöd för denna personuppgiftsbehandling finns i 1 kap. 9 § FRA-PuL. Där föreskrivs att personuppgifter får behandlas av Försvarets radioanstalt om det är nödvändigt för att

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

Motiven finns i prop. 2006/07:46 s. 67 f. Utredningen föreslår att motsvarande bestämmelse införs i den nya lagen.

Vidarebehandling av personuppgifter för vissa andra ändamål än de ursprungliga, får, som nämnts i föregående avsnitt göras med stöd av 1 kap. 6 § 4 p FRA-PuL. Bestämmelsen ger möjlighet att fortsatt behandla insamlade uppgifter så länge personuppgifterna inte behandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in (finalitetsprincipen).

Som utredningen har nämnt i avsnittet om radioanstaltens försvarsunderrättelseverksamhet är det en fördel från integritetsskyddssynpunkt att i görligaste mån precisera i vilka fall personuppgiftsbehandling får ske för andra ändamål än det för vilket uppgifterna har samlats in. En bestämmelse som avser ett sådant ändamål finns i

1 kap. 10 § FRA-PuL. Motiven finns i a. prop. s. 67. Enligt bestämmelsen får personuppgifter behandlas av Försvarets radioanstalt om det är nödvändigt för att biträda andra myndigheter vid värdering, utveckling, anskaffning och drift av signalspaningssystem. Utredningen föreslår att en bestämmelse med denna innebörd tas in i den nya lagen. Den bör dock utformas så att den inte bara tar sikte på värdering, utveckling, anskaffning och drift av signalspaningssystem utan bör få en vidare innebörd. Vidare bör som villkor för biträde till andra myndigheter anges att det kan ges i den utsträckning det följer av lag eller förordning eller regeringsbeslut i ett enskilt fall.

Utredningen föreslår i det följande vissa ytterligare föreskrifter som avser i vilken utsträckning personuppgifter som behandlas för något av ändamålen i utvecklingsverksamheten även ska få behandlas i annan verksamhet inom den egna myndigheten för den verksamhetens behov eller för att lämnas ut till annan för att tillgodose dennes behov.

Som beskrivits i avsnitt 3.3.5 är den information som Försvarets radioanstalt strävar efter att finna och rapportera, i syfte att tillgodose uttryckta underrättelsebehov, ofta konfidentiell och således skyddsvärd för den källa som hanterar informationen. Informationen är därför ofta försedd med någon form av åtkomstskydd för att förhindra obehörig åtkomst. För att framgångsrikt kunna bedriva försvarsunderrättelseverksamhet krävs därför aktuell och ingående kunskap dels om hur signaler förmedlas och hanteras i elektronisk form, dels om de mekanismer som används för att skydda informationen. Personuppgifter som behandlas i Försvarets radioanstalts utvecklingsverksamhet bör därför även få behandlas om det är nödvändigt för att tillhandahålla information som behövs i samverkan med annan avseende utvecklingsverksamhet eller med anledning av samarbete om utvecklingsverksamhet med utländsk underrättelse- eller säkerhetstjänst enligt lagen om signalspaning i försvarsunderrättelseverksamhet.

Eftersom utvecklingsverksamheten syftar till att främja försvarsunderrättelseverksamheten är det inte oförenligt med det ändamål för vilka uppgifterna samlas in att uppgifterna också behandlas i för att tillhandahålla information som behövs i försvarsunderrättelseverksamheten. Detta bör komma till uttryck i lagen.

Utvecklingsverksamheten har också betydelse för Försvarets radioanstalts informationssäkerhetsverksamhet. Även i detta fall är det

inte oförenligt med det ändamål för vilket uppgifterna samlats in att de också behandlas för att tillhandahålla information i den verksamheten. Detta bör komma till uttryck i lagen.

Den föreslagna regleringen innebär således att personuppgiftsbehandling för vissa ändamål uttryckligen regleras i lag, i stället för att, som tidigare, hanteras i enlighet med finalitetsprincipen. Avsikten är att åstadkomma tydlighet i de nu nämnda fallen. Finalitetsprincipen gäller därutöver.

6.3.8 Informationssäkerhetsverksamhet som rättslig grund för behandling av personuppgifter hos Försvarets radioanstalt

Utredningens förslag: Personuppgifter får behandlas i Försvarets radioanstalts informationssäkerhetsverksamhet om det är nödvändigt för att kunna skydda den egna myndigheten eller för att kunna stödja andra verksamheter som är av betydelse för Sveriges säkerhet. Uppgiften att lämna stöd till andra verksamheter ska följa av lag eller förordning eller regeringsbeslut i ett enskilt fall.

Personuppgifter som får behandlas enligt detta ändamål får även behandlas om det är nödvändigt för att tillhandahålla information som behövs

1. i verksamhet hos den som tar emot uppgifter om informationssäkerhet,
2. med anledning av samverkan med andra som verkar på informationssäkerhetsområdet såväl inom som utom landet i den utsträckning det följer av lag eller förordning eller om regeringen i ett enskilt fall beslutar om det,
3. i försvarsunderrättelseverksamheten när det gäller att kartlägga allvarliga yttre hot mot samhällets infrastruktur och främmande underrättelseverksamhet, eller
4. i utvecklingsverksamheten för de ändamål som anges för den verksamheten.

Skäl för utredningens förslag: Av 4 § förordningen med instruktion för Försvarets radioanstalt framgår att Försvarets radioanstalt

har i uppdrag att vara statens resurs för teknisk informationssäkerhet och ska ha hög kompetens inom informationssäkerhetsområdet. Myndigheten får enligt samma bestämmelse efter begäran stödja myndigheter och statligt ägda bolag som hanterar information som bedöms vara känslig från sårbarhetssynpunkt eller i ett säkerhets- eller försvarspolitiskt avseende samt tilldela säkra kryptografiska funktioner till ett antal civila myndigheter och organisationer (se närmare om detta i avsnitt 3.2).

I motiven till FRA-PuL (prop. 2006/07:46 s. 30 f.) anfördes att denna konsultverksamhet främst har rört aktiva it-kontroller, som innebär att Försvarets radioanstalt på uppdragsgivarens begäran söker efter och analyserar brister i säkerheten i datorsystemen. Den information som Försvarets radioanstalt då erhåller bedömdes kunna innehålla personuppgifter, men att Försvarets radioanstalt i så fall, med stöd av ett avtal med uppdragsgivaren, agerar personuppgiftsbiträde vid behandling av dessa personuppgifter. Dessa personuppgifterna skulle således komma att behandlas av Försvarets radioanstalt helt i enlighet med uppdragsgivarens instruktioner och den information som Försvarets radioanstalt får i samband med att uppdraget utförs skulle inte kunna användas i myndighetens försvarsunderrättelse- eller utvecklingsverksamhet. Data innehållande bl.a. personuppgifter återsänds till uppdragsgivaren i samband med slutrapport eller förstörs av Försvarets radioanstalt. Denna beskrivning av konsultverksamheten är enligt utredningens uppfattning fortfarande aktuell. På senare tid har verksamheten utvecklats genom det tekniska detekterings- och varningssystemet (TDV) som beskrivs i avsnitt 3.3.6. Utredningen vill även tillägga att när Försvarets radioanstalt agerar personuppgiftsbiträde sker det inte bara i enlighet med uppdragsgivarens instruktioner utan också enligt de regler som gäller för denne. Vidare kan den information som Försvarets radioanstalt får i samband med att ett uppdrag utförs användas i myndighetens egen verksamhet, om uppdragsgivaren medger det och då sker denna behandling av personuppgifter enligt bestämmelserna för behandling av personuppgifter vid Försvarets radioanstalt.

De personuppgiftsbehandlingar Försvarets radioanstalt genomför som personuppgiftsansvarig inom ramen för informationssäkerhetsverksamheten omfattas inte av FRA-PuL. Utredningen, som tidigare i avsnitt 6.2.3 konstaterat att verksamheten inte omfattas av unionsrätten, anser att det i den nya lagen bör föras in bestämmelser

om behandlingen av personuppgifter i denna verksamhet. Den bör avse den behandling av personuppgifter i informationssäkerhetsverksamheten som är nödvändig för att kunna skydda den egna verksamheten och för att kunna stödja andra verksamheter som är av betydelse för Sveriges säkerhet. Det bör föreskrivas att uppgiften att lämna stöd till andra verksamheter ska följa av lag eller förordning eller regeringsbeslut i ett enskilt fall.

Som utredningen har nämnt i avsnitten om radioanstaltens försvarsunderrättelse- och utvecklingsverksamhet är det en fördel från integritetsskyddssynpunkt att i görligaste mån precisera i vilka fall personuppgiftsbehandling får ske för andra ändamål än det för vilket uppgifterna har samlats in.

Det finns enligt utredningen ett antal tillkommande ändamål för vilka personuppgifter som behandlas i Försvarets radioanstalts informationssäkerhetsverksamhet bör få behandlas. Det bör få ske om det är nödvändigt för att tillhandahålla information som behövs hos den som tar emot uppgifter om informationssäkerhet. Vidare bör det få ske om det är nödvändigt för att tillhandahålla information som behövs med anledning av samverkan med andra som verkar på informationssäkerhetsområdet såväl inom som utom landet. Detta bör dock bara få ske i den utsträckning det följer av lag eller förordning eller om regeringen i ett enskilt fall beslutar om det.

En nära samverkan mellan försvarsunderrättelseverksamheten och informationssäkerhetsverksamheten är av stor betydelse. För underrättelseverksamheten är det angeläget att kunna ta del av uppgifter från informationssäkerhetsverksamheten när det gäller att kartlägga allvarliga yttre hot mot samhällets infrastruktur och främmande underrättelseverksamhet. Personuppgifter bör därför även få behandlas om det är nödvändigt för att tillhandahålla information av detta slag. Försvarets radioanstalt har därvid att förhålla sig till de regler som gäller för försvarsunderrättelseverksamheten.

Informationssäkerhetsverksamheten är även av betydelse för utvecklingsverksamheten. Personuppgifter som får behandlas i informationssäkerhetsverksamheten bör därför även få behandlas om det är nödvändigt för att tillhandahålla information som behövs i utvecklingsverksamheten.

Den föreslagna regleringen innebär således som i de tidigare behandlade fallen att personuppgiftsbehandling för vissa ändamål uttryckligen regleras i lag, i stället för att, som tidigare, hanteras i

enlighet med finalitetsprincipen. Avsikten är att åstadkomma tydlighet i de nu nämnda fallen. Finalitetsprincipen gäller därutöver.

6.3.9 Rättsliga grunder för behandling vid Försvarets radioanstalt av allmänt tillgänglig information för vissa ändamål

Utredningens förslag: Personuppgifter som utgör allmänt tillgänglig information får behandlas av Försvarets radioanstalt om det är nödvändigt för de ändamål som anges för försvarsunderrättelse- och utvecklingsverksamheten och informationssäkerhetsverksamheten.

Skäl för utredningens förslag: Liksom Försvarsmakten (se avsnitt 6.3.4.) bör Försvarets radioanstalt ha ett tydligt stöd för att i s.k. referensdatabaser behandla sådana uppgifter om personer som är allmänt tillgängliga. Det gäller information som utgörs av personuppgifter som kan påträffas vid sökning på internet eller vid sökningar i öppna databaser Uppgifterna kan vara gratis eller tillgängliga på kommersiell grund. Gemensamt för dem är att de är publikt tillgängliga. Det kan röra sig om uppgifter som t.ex. en abonnent på ett eller annat sätt har samtyckt att uppgifterna finns med i elektroniska telefonkataloger eller förteckningar över ip-adresser i olika länder. Utöver de syften för sådan behandling som beskrivs i avsnittet om Försvarsmakten när det gäller försvarsunderrättelseverksamheten, som endast får avse utländska förhållanden, behöver Försvarets radioanstalt behandla personuppgifter i sådana databaser för att kunna filtrera bort signaler i sådana fall där både sändare och mottagare befinner sig i Sverige, t.ex. genom att bedöma vilka ip-adresser som avser datorer i Sverige.

Som tidigare nämnts får enligt 2 a § lagen om signalspaning i försvarsunderrättelseverksamhet inhämtning inte avse signaler mellan en avsändare och en mottagare som båda befinner sig i Sverige. Om sådana signaler inte kan avskiljas redan vid inhämtningen, ska upptagningen eller uppteckningen förstöras så snart det står klart att sådana signaler har inhämtats. Att i en referensdatabas behandla den typen av allmänt tillgängliga personuppgifter kan bidra till att minska antalet sådana inhämtningar.

Även inom utvecklingsverksamheten kan det vara nödvändigt att kunna behandla personuppgifter som utgör allmänt tillgänglig information. Utvecklingsverksamheten syftar till att utveckla och vidmakthålla möjligheterna att bedriva försvarsunderrättelseverksamhet. För detta behöver personuppgifter behandlas t.ex. vid kartläggning av signalmiljön, varvid allmänt tillgänglig information precis som i försvarsunderrättelseverksamheten behöver kunna användas i identifieringssyfte. Även utvecklingsverksamheten omfattas av 2 a § lagen om signalspaning i försvarsunderrättelseverksamhet, varvid behandling av allmänt tillgängliga personuppgifter kan bidra till att minska antalet inhämtningar som ej är tillåtna enligt den bestämmelsen.

Likaså vad gäller informationssäkerhetsverksamheten kan allmänt tillgängliga personuppgifter behöva behandlas. Bland behoven finns möjligheter att identifiera ursprunget till skadlig kod och att löpande kunna bevaka vad som redan är känt avseende sårbarheter i mjuk- och hårdvaror.

I den till lagen anknutna förordningen bör föreskrivas att det för Försvarets radioanstalt får finnas uppgiftssamlingar för allmänt tillgänglig information och att de endast får innehålla information som finns eller har funnits på internet eller i öppna databaser.

Uppgifterna bör vara uppdaterade i enlighet med vad som föreslås i avsnitt 6.4.1.

6.3.10 Rättsliga grunder för behandling för vetenskapliga, statistiska eller historiska ändamål

Utredningens förslag: Försvarsmakten och Försvarets radioanstalt får behandla personuppgifter för vetenskapliga, statistiska eller historiska ändamål inom de föreslagna lagarnas tillämpningsområden.

Skäl för utredningens förslag: Möjligheten att bevara personuppgifter som behandlas automatiserat, för historiska, statistiska eller vetenskapliga ändamål är enligt FM-PuL och FRA-PuL kopplad till regler om gallring. Enligt 6 kap. 1 § i dessa lagar ska personuppgifter gallras så snart uppgifterna inte längre behövs för det ändamål för vilket de behandlas, om inte regeringen eller den myndighet som regeringen bestämmer har meddelat föreskrifter eller i enskilt fall

beslutat att gallring ska ske senast vid viss tidpunkt eller att uppgifter får bevaras för historiska, statistiska eller vetenskapliga ändamål. Enligt 12 § FM-PuF och FRA-PuF har Riksarkivet denna rätt att besluta om bevarande. Ett sådant beslut får till följd att uppgifterna inte gallras.

Utredningen bedömer att det även enligt de nya lagarna bör finnas utrymme att behandla personuppgifter för vetenskapliga, statistiska och historiska ändamål.

6.3.11 Rättsliga grunder för behandling av personuppgifter för att tillgodose behov av information hos enskilda och behov av information vid tillsyn och kontroll

Utredningens förslag: Försvarsmakten och Försvarets radioanstalt får behandla personuppgifter för att kunna tillgodose enskildas behov av information och kunna lämna information vid tillsyn och kontroll.

Skäl för utredningens förslag: Datainspektionen är enligt 10 § FM-PuF och FRA-PuF tillsynsmyndighet enligt FM-PuL och FRA-PuL. Statens inspektion för försvarsunderrättelseverksamheten har enligt sin instruktion till uppgift att kontrollera försvarsunderrättelseverksamheten hos de myndigheter som bedriver sådan verksamhet. Inspektionen är enligt sin instruktion även kontrollmyndighet enligt lagen om signalspaning i försvarsunderrättelseverksamhet. Enligt 10 a § i den lagen är kontrollmyndigheten skyldig att på begäran av en enskild kontrollera om hans eller hennes meddelanden har inhämtats i samband med signalspaning. Det ska här tilläggas att Riksrevisionen, Riksdagens ombudsmän och Justitiekanslern också kan utöva tillsyn.

Något uttryckligt stöd för personuppgiftsbehandling med anledning av en enskilds behov av information eller behov av information vid tillsyn och kontroll finns inte i FM-PuL eller FRA-PuL. Utredningen bedömer emellertid att den personuppgiftsbehandling genom exempelvis sökningar i uppgiftssamlingar och sammanställningar av uppgifter som är nödvändig för att Försvarsmakten och Försvarets radioanstalt ska kunna tillmötesgå enskildas och tillsynsmyndig-

hetens och kontrollmyndighetens behov bör få direkt stöd i de föreslagna lagarna. Utredningen föreslår därför att det i de föreslagna lagarna tas in en bestämmelse om att respektive myndighet får behandla personuppgifter för att kunna tillgodose enskildas behov av information och behovet av information vid tillsyn och kontroll.

Den föreslagna bestämmelsen utgör även den rättsliga grunden för personuppgiftshantering i Försvarsmaktens och Försvarets radioanstalts loggfunktioner i de uppgiftssamlingar som hanterar personuppgifter för de syften som framgår av denna bestämmelse. Bestämmelser om myndigheternas loggfunktioner behandlas i avsnitt 6.6.2.

6.4 Grundläggande krav på behandling av personuppgifter

6.4.1 Grundläggande krav

Utredningens förslag: Försvarsmakten och Försvarets radioanstalt får behandla personuppgifter bara för särskilda, uttryckligt angivna och berättigade ändamål.

Personuppgifter får inte behandlas för något ändamål som är oförenligt med det ändamål för vilket personuppgifterna ursprungligen behandlades.

Personuppgifter ska behandlas författningsenligt och på ett korrekt sätt.

Personuppgifter som behandlas ska vara adekvata och relevanta i förhållande till ändamålen med behandlingen och, om det är nödvändigt, uppdaterade.

Uppgifter som beskriver en persons utseende ska utformas på ett objektivt sätt med respekt för människovärdet.

Fler personuppgifter får inte behandlas än vad som är nödvändigt med hänsyn till ändamålen med behandlingen.

Skäl för utredningens förslag: Av 1 kap. 6 § 1–7 FM-PuL och FRA-PuL framgår att Försvarsmakten respektive Försvarets radioanstalt ska se till att personuppgifter behandlas bara om det är lagligt, att de alltid behandlas på ett korrekt sätt och i enlighet med god sed, att de samlas in bara för särskilda, uttryckligt angivna och berättigade ändamål. Vidare framgår att personuppgifter inte får behandlas för

något ändamål som är oförenligt med det för vilket uppgifterna samlades in, att de är adekvata och relevanta i förhållande till ändamålen med behandlingen. Myndigheterna ska vidare se till att de personuppgifter som behandlas är nödvändiga med hänsyn till ändamålen med behandlingen samt att de är riktiga och, om det är nödvändigt, aktuella. Motiven till bestämmelserna finns i avsnitt 8.4 i prop. 2006/07:46. Utredningen anser att samma föreskrifter bör tas in i de nya lagarna med vissa språkliga justeringar.

En bestämmelse om att uppgifter som beskriver en persons utseende alltid ska utformas på ett objektivt sätt och med respekt för människovärdet finns i FM-PuL (1 kap. 12 § andra stycket andra meningen) och i FRA-PuL (1 kap. 11 § andra stycket andra meningen). Motivet till bestämmelsen finns i prop. 2006/07:46 s. 74 f. Utredningen anser att en sådan föreskrift bör tas in i de nya lagarna.

6.4.2 Behandling av känsliga personuppgifter

Utredningens förslag: Personuppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening eller som rör hälsa, sexualliv eller sexuell läggning får inte behandlas.

När uppgifter om en person behandlas får de dock kompletteras med sådana uppgifter som avses i föregående stycke, om det är absolut nödvändigt för syftet med behandlingen.

Biometriska uppgifter får behandlas endast om det är absolut nödvändigt för ändamålet för behandlingen. Genetiska uppgifter får inte behandlas.

Vid sökning får personuppgifter som avslöjar ras, etniskt ursprung, politiska åsikter. religiös eller filosofisk övertygelse eller medlemskap i fackförening eller som rör hälsa, sexualliv eller sexuell läggning användas som sökbegrepp om det är absolut nödvändigt för syftet med behandlingen. Detsamma gäller biometriska uppgifter.

Skäl för utredningens förslag: Av 1 kap. 12 § FM-PuL och 1 kap. 11 § FRA-PuL framgår att 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 absolut nödvändig med hänsyn till syftet med behandlingen. Vid sökning ska sådana känsliga personuppgifter få användas som sökbegrepp endast om det är absolut nödvändigt med hänsyn till syftet med behandlingen. Motiven till bestämmelserna finns i prop. 2006/07:46 s. 73 f. Utredningen anser att en motsvarande reglering bör införas i de nya lagarna med det tillägget att bestämmelserna även bör gälla sexuell läggning.

Behandling av biometriska och genetiska uppgifter regleras inte i FM-PuL och FRA-PuL.

Med biometriska uppgifter avses enligt den föreslagna definitionen i avsnitt 6.2.9 personuppgifter som rör en fysisk persons fysiska, fysiologiska eller beteendemässiga kännetecken som tagits fram genom särskild teknisk behandling och som möjliggör eller bekräftar unik identifiering av personen i fråga. Försvarsmakten och Försvarets radioanstalt behandlar biometriska uppgifter i sina försvarsunderrättelseverksamheter. Inom signalspaningen får det betraktas som självklart att t.ex. en persons röstprofil, vilket är en biometrisk uppgift, behöver kunna behandlas i identifieringssyfte. Att kunna göra korrekta identifieringar är av avgörande betydelse vid bedömning av källors trovärdighet och informations sakriktighet.

Regeln om att känsliga personuppgifter endast får behandlas såsom komplement till personuppgifter som behandlas på annan grund kan inte tillämpas när det gäller biometriska personuppgifter t.ex. oidentifierade avtryck eller spår. Det finns därför skäl att reglera behandlingen av biometriska uppgifter särskilt. Försvarsmakten och Försvarets radioanstalt bör få behandla biometriska uppgifter om det är absolut nödvändigt för ändamålet med behandlingen. Biometriska uppgifter bör också få behandlas vid sökning om det är absolut nödvändigt för syftet med behandlingen.

Med genetiska uppgifter avses enligt den definition som föreslås i avsnitt 6.2.9 personuppgifter som rör sådana nedärvda eller förvärvade kännetecken för en fysisk person som kan tas fram ur ett prov från personen i fråga. Genetiska uppgifter är av synnerligen integritetskänslig natur. Försvarsmakten och Försvarets radioanstalt har uppgett att de inte har behov av att behandla genetiska uppgifter. Utredningen anser att det av lagstiftningen bör framgå att sådan behandling inte är tillåten.

6.4.3 Behandling av personnummer och samordningsnummer

Utredningens förslag: I den föreslagna lagen om behandling av personuppgifter vid Försvarsmakten tas in en bestämmelse om 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.

Utredningens bedömning: Någon sådan bestämmelse bör inte införas i den föreslagna lagen om behandling av personuppgifter vid Försvarets radioanstalt

Skäl för utredningens förslag och bedömning: En bestämmelse om behandling av personnummer och samordningsnummer finns i 1 kap. 13 § i FM-PuL och 1 kap. 12 § i FRA-PuL. Av bestämmelsen framgår 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.

Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst respektive Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet baserar sig inte på samtycke från den enskilde. Försvarets radioanstalts verksamhet på försvarsunderrättelse- och utvecklingsområdena är inriktad på utländska förhållanden och behandlar därför i liten omfattning personnummer och samordningsnummer. Detsamma kan sägas om informationssäkerhetsverksamheten. Utredningen har konstaterat att en motsvarande reglering inte finns med i förslaget till Säkerhetspolisens datalag. Utredningen anser sig kunna följa det exemplet när det gäller Försvarets radioanstalt.

Även Försvarsmaktens försvarsunderrättelseverksamhet är inriktad på utländska förhållanden och det är, precis som för Försvarets radioanstalt, inte vanligt att personnummer och samordningsnummer behandlas inom denna verksamhet.

För Försvarsmaktens del innebär dock det utökade tillämpningsområdet i förhållande till FM-PuL att myndigheten kommer att

behandla personnummer och samordningsnummer i stor utsträckning, bl.a. beträffande egen personal. Av den anledningen anser utredningen att regleringen bör behållas för Försvarsmakten.

6.4.4 Behandling av personuppgifter om den som uppgifterna rör har offentliggjort uppgifterna eller lämnat sitt samtycke

Utredningens förslag: Utan hinder av vad som föreskrivs i de föreslagna lagarna om känsliga personuppgifter och, såvitt gäller Försvarsmakten, personnummer, får personuppgifter behandlas, om den som personuppgifterna rör har offentliggjort personuppgifterna på ett tydligt sätt. För Försvarsmaktens del ska detta gälla även i det fall samtycke till behandlingen har lämnats av den som uppgifterna rör.

I inget av fallen bör det vara tillåtet att behandla genetiska uppgifter.

Skäl för utredningens förslag: Förslaget till Säkerhetspolisens datalag innehåller bestämmelser om att känsliga personuppgifter får behandlas, om den registrerade har lämnat sitt uttryckliga samtycke till behandlingen eller på ett tydligt sätt har offentliggjort uppgifterna. I FM-PuL och FRA-PuL saknas sådana bestämmelser. Utredningen anser att en motsvarande reglering bör införas i de föreslagna lagarna, dock med den skillnad som framgår av det följande. I Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet och informationssäkerhetsverksamhet blir några samtyckessituationer sällan aktuella, varför någon samtyckesbestämmelse inte behöver finnas för Försvarets radioanstalts del. Detsamma kan sägas om Försvarsmaktens försvarsunderrättelseverksamhet. Däremot kan det förekomma i Försvarsmaktens övriga verksamhet, varför utredningen föreslår att Försvarsmakten får behandla personuppgifter vid de situationer ett samtycke från den som personuppgifterna rör har lämnats.

I inget av fallen bör det vara tillåtet att behandla genetiska uppgifter.

6.4.5 Behandling av personuppgifter i vissa fall

Utredningens förslag: Hantering av information som innebär behandling av personuppgifter ska inte anses oförenlig med bestämmelserna om tillåtlighet, grundläggande krav och känsliga personuppgifter i det skede av behandlingen då det ännu inte har kunnat fastställas vilka personuppgifter som informationen innehåller. En bestämmelse om detta ska föras in i båda lagarna.

Skäl för utredningens förslag: I 1 kap. 13 § FRA-PuL anges 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 ska anses som oförenlig med bestämmelserna om grundläggande krav, ändamål samt behandling av känsliga personuppgifter och personnummer. Så snart det har kunnat fastställas att informationen innehåller personuppgifter måste dock vidare behandling av sådana personuppgifter som förekommer i materialet ske i överenstämmelse med de nämnda bestämmelserna. Någon motsvarighet till 1 kap. 13 § FRA-PuL finns inte i FM-PuL.

Försvarets radioanstalts inhämtning av signaler i tråd ska enligt 3 § lagen om signalspaning i försvarsunderrättelseverksamhet ske automatiserat och det föreskrivs vidare att sådan inhämtning endast får avse signaler som identifierats genom sökbegrepp. Även vid annan inhämtning ska sökbegrepp enligt paragrafen användas för identifieringen av signaler. Detta förfarande reducerar informationsmängden på ett ändamålsenligt sätt före själva inhämtningen och tillvaratar därmed också integritetsskyddsintresset. Behandling av personuppgifter omfattar enligt 1 kap. 4 § FRA-PuL all slags behandling, alltså även den som sker på automatisk väg. Personuppgifter behandlas redan i det tidiga skede när informationen i tillståndsgivna signalbärare genomgår urval med hjälp av sökbegrepp. Det innebär att personuppgiftsbehandling sker även för information som inte inhämtas.

Många av de personuppgifter som behandlas automatiskt blir dessutom aldrig föremål för manuell granskning. Därför är det inte möjligt att veta om de behandlas enligt bestämmelserna i FRA-PuL om grundläggande krav, ändamål, känsliga personuppgifter och personnummer.

I tillämpningen har uppstått frågan om det är först när Försvarets radioanstalt får klart för sig vilka personuppgifter som behandlas som det är möjligt för myndigheten att behandla dem enligt bestämmelserna i 1 kap. 6 och 8–12 §§ FRA-PuL.

I ett tillsynsbeslut den 24 oktober 2016 tog Datainspektionen upp frågan om tolkningen av 1 kap. 13 § FRA-PuL efter det att Statens inspektion för försvarsunderrättelseverksamheten hade anmält frågan dit. Datainspektionen kom fram till att varken bestämmelsens ordalydelse eller förarbetena till FRA-PuL ger stöd för en sådan tolkning som anges ovan. Inspektionen konstaterade vidare att bestämmelsen enligt sin ordalydelse i praktiken inte går att förena med inhämtning genom signalspaning på det sätt som det förefaller ha förutsetts genom införandet av lagen om signalspaning. Det var enligt Datainspektionen således uppenbart att bestämmelsen inte är anpassad till för de behov och förutsättningar som gäller för Försvarets radioanstalts verksamhet i dag. Frågan om hur bestämmelsen ska tolkas borde enligt Datainspektionen ha tagits upp vid införandet av lagen om signalspaning.

Det var Datainspektionens uppfattning att bestämmelsen behöver ses över och anpassas till det mandat lagstiftaren har gett Försvarets radioanstalt genom lagen om signalspaning. Datainspektionen fann mot den angivna bakgrunden anledning att uppmärksamma regeringen på detta behov och sände en kopia av beslutet till Försvarsdepartementet.

Utredningen kan konstatera att bestämmelsen enligt sin ordalydelse innebär att den inte undantar tillämpning av de nämnda föreskrifterna om grundläggande krav, ändamål, känsliga personuppgifter och personnummer i de fall då man redan från början vet att informationen innehåller personuppgifter. Praktiskt taget all information som innehållande kommunikation mellan människor som Försvarets radioanstalt inhämtar innehåller personuppgifter. Innan uppgifterna har översatts, forcerats och bedömts av analytiker är det okänt vilka specifika personuppgifter som behandlas. Många av de personuppgifter som behandlas på automatisk väg blir aldrig föremål för manuell granskning. Det är därför en omöjlighet för Försvarets radioanstalt att, såvida inte en analytiker bearbetat och bedömt personuppgifterna, hävda att personuppgifterna har behandlats i enlighet med bestämmelserna om grundläggande krav, ändamål, känsliga personuppgifter och personnummer.

Som Datainspektionens beslut ger uttryck för står bestämmelsen därmed i konflikt med den personuppgiftsbehandling som lagen om signalspaning i försvarsunderrättelseverksamhet förutsätter ska ske hos Försvarets radioanstalt efter inhämtningsskedet. Utredningen föreslår därför att bestämmelsen utformas så att den tar sikte på det skede då det inte har kunnat fastställas vilka personuppgifterna är. Den närmare utformningen bör anpassas till den föreslagna lagen om behandling av personuppgifter vid Försvarets radioanstalt.

Även i Försvarets radioanstalts informationssäkerhetsverksamhet förekommer personuppgifter. Vilka dessa är kan visa sig först i ett senare skede av hanteringen. Den föreslagna bestämmelsen kommer att medge hantering av information som innebär behandling av personuppgifter i ett tidigt skede då det inte har kunnat fastställas vilka personuppgifterna är.

Motsvarande behov av legala förutsättningar för behandling av material innan det är klarlagt vilka personuppgifter materialet innehåller finns även hos Försvarsmakten. Exempel på sådana situationer anges i det följande.

För att Försvarsmakten ska kunna bedriva en effektiv verksamhet är det nödvändigt att använda sig av information som t.ex. delges till Försvarsmakten av andra myndigheter. När sådan information tas in i myndighetens tekniska system är det inte möjligt för Försvarsmakten att i förväg veta vad som rapporteras och vilka personuppgifter som förekommer i handlingen. Det är därför heller inte möjligt att i förekommande fall veta om personuppgifterna behandlas enligt bestämmelserna om grundläggande krav.

När Försvarsmakten får in en rapport från en annan myndighet som rör försvarsunderrättelseverksamhet eller militär säkerhetstjänst tas denna rapport normalt in i Försvarsmaktens informationssystem för underrättelse- och säkerhetstjänsten. I samband med att rapporten läses in i systemet och diarieförs görs en notering om det förekommer personuppgifter i handlingen. Detsamma gäller om Försvarsmakten får in en handling om exempelvis försvarsplanering. Rapporten läses in i Försvarsmaktens informationssystem för ärendehantering. Någon prövning utifrån bestämmelserna om grundläggande krav, tillåtlighet och känsliga personuppgifter görs dock inte förrän personuppgifterna bearbetas i respektive verksamhet. Det är först när personuppgifterna behandlas i verksamheten som en bedömning kan göras om de är nödvändiga för densamma.

6.4.6 Längsta tid som personuppgifter får behandlas

Utredningens förslag: Personuppgifter som behandlas automatiserat får inte behandlas under längre tid än vad som behövs för något eller några av de ändamål för vilka Försvarsmakten eller Försvarets radioanstalt enligt de föreslagna lagarna får behandla personuppgifter.

I lagarna tas in en upplysningsföreskrift om att regeringen eller den myndighet regeringen bestämmer kan meddela föreskrifter eller i ett enskilt fall besluta att personuppgifter får behandlas endast under viss tid eller bevaras för historiska, statistiska eller vetenskapliga ändamål.

Skäl för utredningens förslag: Hur länge personuppgifter får bevaras enligt FM-PuL och FRA-PuL regleras i bestämmelserna om gallring i 6 kap. 1 § FM-PuL och FRA-PuL. Av bestämmelserna framgår att personuppgifter som behandlas automatiserat ska gallras så snart uppgifterna inte längre behövs för det ändamål för vilket de behandlas, om inte regeringen eller den myndighet som regeringen bestämmer har meddelat föreskrifter eller i enskilt fall beslutat att gallring ska ske senast vid viss tidpunkt eller att uppgifter får bevaras för historiska, statistiska eller vetenskapliga ändamål.

Utredningen anser att samma reglering bör gälla i de föreslagna lagarna med en viss språklig justering som bl.a. innebär att uttrycket gallring inte används. I stället föreslås en föreskrift om längsta tid som personuppgifter får behandlas. Bestämmelsen hindrar inte att Försvarsmakten och Försvarets radioanstalt arkiverar och bevarar allmänna handlingar eller lämnar arkivmaterial till en arkivmyndighet.

Förordningsföreskrifter för Försvarsmakten

I den förordning som ska knyta an till den föreslagna lagen om behandling av personuppgifter vid Försvarsmakten bör tas in föreskrifter om bevarande av personuppgifter i uppgiftssamlingar i försvarsunderrättelseverksamheten och den militära säkerhetstjänsten och som finns i rapportunderlag och underrättelserapporter. Om dessa personuppgifter inte längre behövs för de ändamål för vilka de

behandlas, ska de enligt utredningens förslag bevaras för historiska, statistiska eller vetenskapliga ändamål.

I FM-PuF finns bestämmelser om uppgiftssamlingar för försvarsunderrättelsetjänst, säkerhetsunderrättelsetjänst, säkerhetsskyddstjänst och signalkontroll. En redovisning av dem finns i avsnitt 5.1.5. I avsnitt 5.1.12 redovisas föreskrifter om gallring, såvitt avser uppgiftssamlingarna för säkerhetsunderrättelsetjänst, säkerhetsskyddstjänst och signalkontroll. Huvudregeln innebär att personuppgifter ska gallras när de inte längre behövs för det ändamål för vilket de behandlas. Datainspektionen har pekat på att det ska vara en fortlöpande prövning om en personuppgift ska behandlas eller inte. Det är därför heller inte av integritetsskyddsskäl nödvändigt med särskilda gallringsfrister inom delar av den militära säkerhetstjänsten. Där kan personuppgifter i likhet med vad som är fallet i försvarsunderrättelseverksamheten behöva behandlas under mycket lång tid. I den förordning som knyter an till lagen föreslår utredningen därför inga tidsfrister för behandlingen av personuppgifter i uppgiftssamlingarna för säkerhetsunderrättelsetjänst och för säkerhetsskydd. Personuppgifter i en uppgiftssamling för signalkontroll får dock inte behandlas längre än ett år efter det att behandlingen påbörjades. Detta innebär igen ändring.

Utredningen föreslår vidare att det i förordningen tas in ett bemyndigande för Riksarkivet att, efter samråd med Försvarsmakten, meddela föreskrifter om att personuppgifter som inte längre får behandlas ska bevaras.

Förordningsföreskrifter för Försvarets radioanstalt

Enligt 4 § FRA-PuF ska det vid Försvarets radioanstalt finnas uppgiftssamlingar för underrättelser som innehåller personuppgifter. Uppgiftssamlingarna får endast innehålla färdiga underrättelserapporter. I den förordning som ska knyta an till den föreslagna lagen föreslår utredningen att uppgiftssamlingarna för underrättelser även får innehålla rapportunderlag. Utredningen återkommer till den frågan i avsnitt 6.5.1. När personuppgifter i rapportunderlag och underrättelserapporter inte längre behövs för de ändamål för vilka de behandlas ska de enligt utredningens förslag bevaras för historiska, statistiska eller vetenskapliga ändamål.

I FRA-PuF finns bestämmelser om uppgiftssamlingar för bl.a. råmaterial, information om signalmiljön och företeelser mot vilka signalspaningen inriktas (2, 5 och 6 §§). I bestämmelserna finns föreskrifter om gallring. En redovisning av dem finns i avsnitt 5.1.12.

I den förordning som ska knyta an till lagen om behandling av personuppgifter vid Försvarets radioanstalt föreslår utredningen föreskrifter när det gäller hur länge uppgifter får behandlas. Personuppgifter i en uppgiftssamling för råmaterial får inte behandlas längre än ett år efter det att behandlingen påbörjades. Detta innebär ingen ändring.

När det gäller uppgiftssamlingar för information om signalmiljön och företeelser mot vilka signalspaningen inriktas föreslår utredningen av samma anledning som nyss redovisats beträffande den militära säkerhetstjänsten däremot inga särskilda tidsfrister för behandlingen.

Utredningen föreslår vidare att det i förordningen tas in ett bemyndigande för Riksarkivet att, efter samråd med Försvarets radioanstalt, meddela föreskrifter om att personuppgifter som inte längre får behandlas ska bevaras. Detta ska dock inte gälla uppgiftssamlingar för råmaterial.

6.4.7 Försvarsmaktens utlämnande av personuppgifter

Utredningens förslag: Personuppgifter som behandlas med stöd av den föreslagna lagen får föras över till andra länder eller internationella organisationer endast om sekretess inte hindrar det och det är nödvändigt för att Försvarsmakten ska kunna fullgöra sina uppgifter inom ramen för det internationella försvars- och säkerhetssamarbetet.

Regeringen kan meddela föreskrifter eller i enskilt fall besluta att överföring får ske även i andra fall, om det är nödvändigt för verksamheten vid Försvarsmakten.

Försvarsmakten får lämna ut personuppgifter elektroniskt på annat sätt än genom direktåtkomst, om det inte är olämpligt. Regeringen kan meddela föreskrifter som begränsar denna möjlighet.

Elektroniskt utlämnande genom direktåtkomst är tillåtet bara i den utsträckning som anges i den föreslagna lagen.

Skäl för utredningens förslag:

Utlämnande till andra länder

Enligt 1 kap. 17 § FM-PuL får personuppgifter som behandlas med stöd av den lagen föras över till andra länder eller mellanfolkliga organisationer endast om sekretess inte hindrar det och det är nödvändigt för att Försvarsmakten ska kunna fullgöra sina uppgifter inom ramen för det internationella försvarsunderrättelse- och säkerhetssamarbetet, om inte regeringen meddelat föreskrifter eller i ett enskilt fall beslutat om att överföring får ske även i andra fall då det är nödvändigt för verksamheten i Försvarsmakten. Motiven finns i prop. 2006/07:46 s. 80 f. Det kan här erinras om bestämmelsen i 3 § förordningen om försvarsunderrättelseverksamhet. Enligt den bestämmelsen får de myndigheter som bedriver försvarsunderrättelseverksamhet samarbeta i underrättelsefrågor med andra länder och internationella organisationer endast under förutsättning att syftet med samarbetet är att tjäna den svenska statsledningen och det svenska totalförsvaret. De uppgifter som myndigheterna lämnar till andra länder och internationella organisationer får inte vara till skada för svenska intressen. Vad som avses med svenska intressen anges inte närmare. I tillämpningen har utöver svenska statens intressen även avsetts intressen hos svenska företag och enskilda.

Utredningen anser att en bestämmelse som motsvarar 1 kap. 17 § FM-PuL bör tas in i den nya lagen. Med hänsyn till det vidgade tillämpningsområdet för behandlingen av personuppgifter vid Försvarsmakten bör dock ”försvarsunderrättelse- och säkerhetssamarbetet” ersättas med ”försvars- och säkerhetssamarbetet”.

Elektroniskt utlämnande

Enligt 1 kap. 14 § FM-PuL får endast enstaka personuppgifter lämnas ut på medium för automatiserad behandling, om inte regeringen har meddelat föreskrifter eller i ett enskilt fall beslutat om att uppgifter får lämnas ut på sådant medium även i andra fall. Motiven finns i prop. 2006/07:46 s. 77 f.

I princip anses allt elektroniskt utlämnande som inte görs genom direktåtkomst utlämnat på medium för automatiserad behandling. Sådant utlämnande kan göras på många olika sätt. Det kan vara fråga

om att personuppgifter lämnas t.ex. via e-post eller dvd-skiva eller genom direkt överföring från ett datasystem till ett annat via elektroniska kommunikationsnät.

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. Detta innebär effektivitetsvinster för mottagaren, samtidigt som det kan innebära risker för den personliga integriteten. Regeringen ansåg därför i motiven till bestämmelsen i FM-PuL att möjligheten till utlämnande av personuppgifter på medium för automatiserad behandling skulle vara begränsad (prop. 2006/07:46 s. 78).

Regeringen har utnyttjat bemyndigandet att meddela föreskrifter genom att föreskriva att utlämnande på medium för automatiserad behandling får omfatta fler än enstaka uppgifter, om uppgifterna lämnas ut till en annan statlig myndighet (7 § FM-PuF).

Elektroniskt utlämnande ger effektivitetsvinster

Myndigheter som arbetar med bl.a. underrättelse- och säkerhetsverksamhet har stora behov av att kommunicera med andra myndigheter. Det kan röra sig om att både begära, lämna eller utbyta information. Huvuddelen av all lagring och kommunikation av information sker numera elektroniskt på olika sätt som ger effektivitetsvinster, vilket som angetts ovan även uppmärksammats vid tillkomsten av FM-PuL och FRA-PuL.

I takt med den generella utvecklingen av informationstekniken har även myndigheters möjligheter att på olika sätt dela och ta del av information ökat. Informationshanteringsutredningen, som hade i uppdrag att generellt se över frågor om elektroniskt utlämnande, framhöll att frågan om hur den bästa effektiviteten kan uppnås för närvarande inte synes handla så mycket om vilken elektronisk utlämnandeform som bör väljas utan mer om myndigheternas möjlighet att överhuvudtaget åstadkomma det informationsutbyte som regeringen eller de själva vill ska förekomma. Problemen med att uppnå önskad effektivisering förefaller enligt den utredningen till viss del handla om legala förutsättningar för ett visst informationsutbyte (SOU 2015:39 s. 148).

Risker med elektroniskt utlämnande

Utlämnande av personuppgifter på medium för automatiserad behandling medför risker från integritetssynpunkt. Sådant utlämnande innebär nämligen som regel att mottagaren kan bearbeta informationen, t.ex. genom att samköra den mot elektroniska uppgifter som har hämtats från andra informationskällor. Det ökar risken för att uppgifterna behandlas i strid med de grundläggande kraven på dataskydd. I detta sammanhang bör emellertid beaktas att en begränsning av möjligheter att överföra information elektroniskt i praktiken får begränsad betydelse eftersom modern teknik enkelt kan omvandla text på papper till elektroniska uppgifter.

Bestämmelserna om elektronisk informationsöverföring behöver moderniseras

I förslaget till Säkerhetspolisens datalag föreslås att personuppgifter får lämnas ut elektroniskt på annat sätt än genom direktåtkomst, om det inte är olämpligt (1 kap. 19 §). Det anges vidare att regeringen kan meddela föreskrifter som begränsar möjligheten att lämna ut personuppgifter på det sättet (1 kap. 22 § 2).

I motiven till förslaget anges effektivitetsskäl. Det anförs att även om det förekommer integritetskänsliga uppgifter måste riskerna med att överföra sådana uppgifter elektroniskt vägas mot behovet av en snabb och effektiv säker kommunikation (SOU 2017:74 s. 374).

Sättet att hantera stora volymer information, inbegripet personuppgifter, har genomgått stora förändringar sedan tillkomsten av FM-PuL. Huvuddelen av all informationsöverföring mellan Försvarsmakten och andra myndigheter sker i dag elektroniskt, vilket talar för att behandlingen huvudsakligen bör regleras direkt i lag. I likhet med vad som har föreslagits när det gäller Säkerhetspolisens behandling av personuppgifter anser utredningen att Försvarsmakten bör kunna få lämna ut personuppgifter elektroniskt på annat sätt än genom direktåtkomst, om det inte är olämpligt. Utredningen anser i likhet med vad som föreslås för Säkerhetspolisen att regeringen kan meddela föreskrifter som begränsar möjligheten att lämna ut personuppgifter på annat sätt än genom direktåtkomst.

Bestämmelser om direktåtkomst behandlas särskilt i avsnitt 6.5.2.

6.4.8 Försvarets radioanstalts utlämnande av personuppgifter

Utredningens förslag: Personuppgifter som behandlas med stöd av den föreslagna lagen får föras över till en utländsk underrättelse- eller säkerhetstjänst, en utländsk organisation inom informationssäkerhetsområdet eller en internationell organisation endast om sekretess inte hindrar det och det är nödvändigt för att Försvarets radioanstalt ska kunna fullgöra sina uppgifter inom ramen för det internationella försvarsunderrättelse- och säkerhetssamarbetet.

Regeringen kan meddela föreskrifter eller i enskilt fall besluta att överföring får ske även i andra fall då det är nödvändigt för verksamheten vid Försvarets radioanstalt.

Personuppgifter får lämnas ut elektroniskt på annat sätt än genom direktåtkomst, om regeringen har meddelat föreskrifter eller särskilt beslutat om det.

Elektroniskt utlämnande genom direktåtkomst är tillåtet bara i den utsträckning som anges i den föreslagna lagen.

Skäl för utredningens förslag: Enligt 1 kap. 17 § FRA-PuL får personuppgifter som behandlas enligt den lagen föras över till andra länder eller mellanfolkliga organisationer endast om sekretess inte hindrar det och det är nödvändigt för att Försvarets radioanstalt ska kunna fullgöra sina uppgifter inom ramen för det internationella försvarsunderrättelse- och säkerhetssamarbetet, om inte regeringen. har meddelat föreskrifter eller i ett enskilt fall beslutat att överföring får ske även i andra fall då det är nödvändigt för verksamheten vid Försvarets radioanstalt. Motiven finns i prop. 2006/07:47 s. 80 f.

I den föreslagna lagen bör enligt utredningens mening en motsvarande föreskrift tas in. Dock bör den krets till vilken överföringen får ske anges vara utländsk underrättelse- eller säkerhetstjänst, en utländsk organisation inom informationssäkerhetsområdet eller en internationell organisation. I den förordning som ska knyta an till lagen bör föreskrivas att personuppgifter får föras över i sådana fall, om överföringen tjänar den svenska statsledningen eller det svenska totalförsvaret och att överföringen av uppgifter inte får vara till skada för svenska intressen. Som tidigare nämnts har i tillämpningen som svenska intressen avsetts, utöver svenska statens intressen, även intressen hos svenska företag och enskilda.

Enligt 1 kap. 14 § FRA-PuL får endast enstaka personuppgifter lämnas ut på medium för automatiserad behandling, om inte regeringen har meddelat föreskrifter eller i ett enskilt fall beslutat att uppgifter får lämnas på sådant medium i andra fall. Motiven finns i prop. 2006/07:46 s. 77 f. I 8 § FRA-PuF har regeringen föreskrivit att utlämnande på medium för automatiserad behandling får omfatta fler än enstaka uppgifter, om uppgifterna lämnas ut till en annan statlig myndighet. Som tidigare nämnts finns liknande bestämmelser för Försvarsmakten i FM-PuL och FM-PuF.

Utredningen har, som framgått, för Försvarsmaktens del föreslagit en bestämmelse som innebär att utlämnande elektroniskt på annat sätt än genom direktåtkomst får ske, om det inte är olämpligt. Som utredningen konstaterat där har en liknande bestämmelse tagits in i förslaget till Säkerhetspolisens datalag. Skäl för en sådan bestämmelse kan även anföras när det gäller Försvarets radioanstalt. Arten av och antalet uppgifter som det är fråga om vid Försvarets radioanstalt gör att integritetsskyddsaspekterna enligt utredningens mening emellertid talar för en mer restriktiv lagreglering. Till skillnad mot Försvarsmakten har Försvarets radioanstalt inte heller önskat någon förändring av bestämmelsen.

Utredningen föreslår att det i den föreslagna lagen tas in en föreskrift enligt vilken personuppgifter får lämnas ut elektroniskt på annat sätt än genom direktåtkomst, om regeringen har meddelat föreskrifter eller särskilt beslutat om det. I förordningen till lagen bör regeringen föreskriva att personuppgifter får lämnas ut till statliga myndigheter på annat sätt än genom direktåtkomst. Den föreslagna regleringen blir därmed lika restriktiv som den nuvarande.

6.5 Gemensamt tillgängliga uppgifter

6.5.1 Personuppgifter som får göras gemensamt tillgängliga

Utredningens förslag: Särskilda bestämmelser ska gälla för behandling av personuppgifter som görs eller har gjorts gemensamt tillgängliga. Dessa bestämmelser samlas i ett eget kapitel i respektive lag.

Försvarsmakten
Personuppgifter får göras gemensamt tillgängliga om det behövs för något av de ändamål för vilka Försvarsmakten får behandla personuppgifter. Personuppgifter som görs gemensamt tillgängliga inom Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst ska även fortsättningsvis behandlas i uppgiftssamlingar.

Personuppgifter som endast ett fåtal personer har tillgång till ska inte anses som gemensamt tillgängliga.

Regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter eller beslut i enskilda fall vilka uppgiftssamlingar som får finnas och vilka uppgifter som får behandlas i respektive uppgiftssamling.

Försvarets radioanstalt
Personuppgifter får göras gemensamt tillgängliga och behandlas i uppgiftssamlingar om det behövs för något av de ändamål som anges i lagen.

Personuppgifter som endast ett fåtal personer har tillgång till anses inte som gemensamt tillgängliga.

Regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter eller beslut i enskilda fall vilka uppgiftssamlingar som får finnas och vilka uppgifter som får behandlas i respektive uppgiftssamling.

Skäl för utredningens förslag: Enligt 1 kap. 4 § FM-PuL och FRA-PuL är en uppgiftssamling en samling med uppgifter som med hjälp av automatiserad behandling används gemensamt. Enligt 1 kap. 7 § FM-PuL och FRA-PuL får, under de förutsättningar som anges i

dessa lagar, personuppgifter behandlas i uppgiftssamlingar för Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst samt Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet. Enligt bestämmelserna får regeringen meddela föreskrifter eller beslut i enskilda fall om vilka uppgiftssamlingar som får finnas och vilka uppgifter som får behandlas i respektive samling. Motiven finns i prop. 2006/07:46 s. 59 f.

Avgörande för när automatiserat behandlade uppgifter ska anses ingå i en uppgiftssamling är enligt förarbetena att uppgifterna används gemensamt av Försvarsmakten eller Försvarets radioanstalt i en viss verksamhet för de ändamål som ska styra behandlingen av uppgifter inom verksamheten. När en handläggare arbetar med ordbehandling lagras uppgifter elektroniskt på hårddisken i en dator eller i en server hos Försvarsmakten eller Försvarets radioanstalt. Uppgiften är då normalt åtkomlig endast för handläggaren själv och 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 ska 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.

Gemensamt tillgängliga uppgifter – ny reglering

Utöver de bestämmelser som behandlats ovan angående uppgiftssamlingar finns inte i FM-PuL och FRA-PuL några bestämmelser som reglerar behandling av personuppgifter som görs eller har gjorts gemensamt tillgängliga. Sådana bestämmelser finns i förslaget till Säkerhetspolisens datalag (SOU 2017:74). Med gemensamt tillgängliga uppgifter avses enligt dessa bestämmelser uppgifter som inte enbart ett fåtal har tillgång till.

Liksom i förslaget till Säkerhetspolisens datalag bör regleringen om gemensamt tillgängliga uppgifter finnas i ett särskilt kapitel i respektive lag. Det bör enligt utredningen finnas en tydlig koppling till de tillåtna rättsliga grunderna för personuppgiftsbehandling. Detta innebär tydliga regler och underlättar den bedömning som ska ske vid tillsyn och kontroll om huruvida behandlingen av personuppgifter vilar på rättslig grund.

En grundläggande förutsättning för att personuppgifter ska anses vara gemensamt tillgängliga är att de kan användas gemensamt av flera, dvs. att fler än en person har åtkomst till uppgifterna. Uppgifter som endast ett fåtal personer har rätt att ta del av bör dock inte anses som gemensamt tillgängliga.

Försvarsmakten och Försvarets radioanstalt bör kunna samarbeta med andra, företrädesvis myndigheter, och inom ramen för sådant samarbete behandla personuppgifter i gemensamma projekt. Bland annat för att möjliggöra ett sådant samarbete görs bedömningen i avsnitten 6.5.2 och 6.5.3 att vissa myndigheter bör kunna medges direktåtkomst till uppgifter som har gjorts gemensamt tillgängliga inom Försvarsmakten och Försvarets radioanstalt. Syftet med att begränsa åtkomsten till gemensamt tillgängliga uppgifter är att personuppgifter – och behandlingen av sådana uppgifter – bör kringgärdas av ett extra skydd när de sprids till andra myndigheter än Försvarsmakten och Försvarets radioanstalt. Konsekvensen av begränsningen blir att bestämmelserna om gemensamt tillgängliga uppgifter alltid blir tillämpliga i projekt med deltagare från andra myndigheter, oavsett antalet deltagare i projektet.

Liksom angavs i lagstiftningsarbetet vid tillkomsten av FM-PuL och FRA-PuL, anser utredningen att det inte är möjligt att i lagstiftningen ange någon exakt gräns för när en viss behandling ska 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 handläggare inom Försvarsmakten 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 eller annat program där han eller hon ensam behandlar personuppgiften. Den personuppgiftsansvarige har emellertid ett ansvar för att gränsdragningsproblem inte uppstår på grund av brister i den tekniska utformningen av ett datorsystem. Genom de höga säkerhetskrav som omgärdar Försvarsmaktens och Försvarets radioanstalts informationssystem är det också nödvändigt att inom verksamheten ha klart för sig huruvida en viss uppgift ingår i en uppgiftssamling eller inte.

Den närmare regleringen av vilka kategorier av uppgifter som ska få behandlas bör även fortsättningsvis huvudsakligen regleras i förordning eller genom regeringsbeslut.

För att undvika en alltför detaljerad reglering i lag bör regeringen meddela närmare föreskrifter eller beslut i enskilda fall om vilka uppgiftssamlingar som får finnas och vilka uppgifter som får behandlas i respektive samling.

Närmare om Försvarsmakten

Inom ramen för den personuppgiftsbehandling som sker av Försvarsmakten i försvarsunderrättelseverksamheten och den militära säkerhetstjänsten är risken för integritetsintrång för den enskilde typiskt sett större än vid annan personuppgiftsbehandling som omfattas av förslaget till lag om behandling av personuppgifter vid Försvarsmakten. Det finns därför enligt utredningen skäl att även fortsättningsvis reglera behandling av personuppgifter i uppgiftssamlingar i dessa verksamheter i lag. Beträffande personuppgiftsbehandling utanför försvarsunderrättelseverksamheten och den militära säkerhetstjänsten gör utredningen emellertid följande bedömning.

I stort sett samtliga personuppgifter som behandlas av Försvarsmakten i de andra verksamheterna är av sådan karaktär att de kan betraktas som gemensamt tillgängliga. De uppgifter som personal hos Försvarsmakten har tillgång till begränsas dock genom krav på behörighet. Åtkomsten begränsas såtillvida att de som har behörighet endast får tillgång till de delar av informationssystemen som de behöver för att kunna fullgöra sina arbetsuppgifter. Inloggning i Försvarsmaktens huvudsystem för ärendehantering, FM AP kan till exempel endast ske med hjälp av totalförsvarets elektroniska id-kort. Aktiviteter i systemen loggas och logguppföljning görs regelbundet av it-säkerhetschefen och verksamhetschefen.

Personuppgiftsbehandlingen inom ramen för lagförslaget omgärdas av särskilda skyddsregler. Personuppgiftsbehandlingen kommer exempelvis att begränsas genom bestämmelser om lagens tillämpningsområde och särskilda ändamålsbestämmelser, om att tillgången till personuppgifter ska begränsas till vad varje anställd behöver för att kunna fullgöra sina arbetsuppgifter. En begränsning följer också av att det föreslås en särskild reglering för när och hur direktåtkomst för andra aktörer får medges. Lagen föreslås även innehålla bestämmelser om sökförbud. På detta sätt begränsas risken för otillbörlig spridning av uppgifterna.

Mot denna bakgrund utgör de föreslagna skyddsreglerna ett tillräckligt integritetsskydd för den uppgiftsbehandling som omfattas av lagförslaget och som sker vid Försvarsmakten utanför försvarsunderrättelseverksamheten och den militära säkerhetstjänsten. Något behov av en mer restriktiv särreglering finns därför inte. För behandling av personuppgifter avseende de nya ändamålen bör därför Försvarsmakten få bestämma om uppgiftssamlingar ska införas och vad de i så fall ska innehålla. Detta bör anges i den nya förordningen om behandlingen av personuppgifter vid Försvarsmakten.

I den förordning som ska knyta an till den föreslagna lagen föreslås följande när det gäller uppgiftssamlingar hos Försvarsmakten.

Vid Försvarsmakten får det finnas uppgiftssamlingar för försvarsunderrättelseverksamhet som innehåller personuppgifter. Uppgiftssamlingarna år endast innehålla uppgifter som är nödvändiga för att Försvarsmakten ska kunna bedriva verksamhet enligt lagen (2000:130) om försvarsunderrättelseverksamhet.

En uppgiftssamling för försvarsunderrättelseverksamhet får endast innehålla

1. identifieringsuppgifter,
2. uppgifter om de omständigheter och händelser som ger anledning att anta att den som behandlingen rör har betydelse för försvarsunderrättelseverksamheten,
3. upplysningar om varifrån uppgiften kommer och om en uppgiftslämnares trovärdighet, och
4. allmänt tillgänglig information som finns på internet eller i öppna databaser.

När personuppgifter som avses ovan och som finns i rapportunderlag och underrättelserapporter inte längre behövs för de ändamål för vilka de behandlas, ska de bevaras för historiska, statistiska eller vetenskapliga ändamål.

Vid Försvarsmakten får det finnas uppgiftssamlingar för säkerhetsunderrättelsetjänst som innehåller personuppgifter. Uppgiftssamlingarna får endast innehålla uppgifter som är nödvändiga för att upptäcka och klarlägga säkerhetshotande verksamhet som riktas mot Försvarsmakten och dess säkerhetsintressen samt allmänt tillgänglig information som finns på internet eller i öppna databaser.

När personuppgifter som avses ovan och som finns i rapportunderlag och underrättelserapporter inte längre behövs för de ändamål för vilka de behandlas, ska de bevaras för historiska, statistiska eller vetenskapliga ändamål.

Vid Försvarsmakten får det finnas uppgiftssamlingar för säkerhetsskyddstjänst som innehåller personuppgifter. Uppgiftssamlingarna får endast innehålla uppgifter som är nödvändiga för att förebygga och avvärja säkerhetshotande verksamhet som riktas mot Försvarsmakten och dess säkerhetsintressen.

Vid Försvarsmakten får det finnas uppgiftssamlingar för signalkontroll som innehåller personuppgifter. Uppgiftssamlingarna får endast innehålla uppgifter som är nödvändiga för att förhindra obehörig insyn i och påverkan av totalförsvarets telekommunikations- och informationssystem.

I avsnitt 6.4.6 föreslår utredningen inga tidsfrister för behandlingen av personuppgifter i uppgiftssamlingarna för säkerhetsunderrättelsetjänst och för säkerhetsskydd. Personuppgifter i en uppgiftssamling för signalkontroll föreslås, i likhet med vad som nu gäller, inte få behandlas längre än ett år efter det att behandlingen påbörjades.

Närmare om Försvarets radioanstalt

På samma sätt som för Försvarsmakten föreslås för Försvarets radioanstalts behandling av personuppgifter ett kapitel om personuppgifter som får göras gemensamt tillgängliga. Enligt förslaget till ny reglering bör personuppgifter få göras gemensamt tillgängliga och behandlas i uppgiftssamlingar om det behövs för något av de syften som anges i lagens andra kapitel. Således omfattas, utöver försvarsunderrättelse- och utvecklingsverksamheten, även informationssäkerhetsverksamheten av den nya regleringen.

I den förordning som ska knyta an till lagen om behandling av personuppgifter vid Försvarets radioanstalt föreslår utredningen följande förändringar när det gäller uppgiftssamlingar. Enligt 3 § FRA-PuF ska rapportunderlag finnas i uppgiftssamlingar för analyser. Uppgiftssamlingarna för underrättelser får enligt utredningens förslag innehålla rapportunderlag på grund av det nära sambandet mellan rapportunderlag och underrättelserapporter. Då analyser och

bedömningar i underrättelserapporter bygger på information i rapportunderlagen är det logiskt att underlagen behandlas enligt samma regler som de resulterande underrättelserapporterna.

När personuppgifter i rapportunderlag och underrättelserapporter inte längre behövs för de ändamål för vilka de behandlas ska de bevaras för historiska, statistiska eller vetenskapliga ändamål. Därmed säkerställs bl.a. möjligheterna att i ljuset av ny information vid behov ompröva tidigare analyser och bedömningar. Detta torde vara ett grundläggande krav på all underrättelserapportering som kan ligga till grund för sådana aktiviteter som rapportmottagarna kan komma att genomföra baserade på rapporteringen.

Vid Försvarets radioanstalt får det finnas uppgiftssamlingar för informationssäkerhetsverksamhet som innehåller personuppgifter. De får endast innehålla information om uppdragsgivare, information som rör it-angrepp samt bearbetningsunderlag och analysresultat.

Vidare får det finnas uppgiftssamlingar för allmänt tillgänglig information som innehåller personuppgifter. De får endast innehålla information som finns eller har funnits på internet eller i öppna databaser.

Slutligen får det finnas uppgiftssamlingar för loggar som förs med stöd av bestämmelser i den föreslagna lagen.

6.5.2 Direktåtkomst till personuppgifter hos Försvarsmakten

Utredningens förslag: Säkerhetspolisen och Försvarets radioanstalt får medges direktåtkomst till personuppgifter som utgör bearbetningsunderlag och analysresultat inom försvarsunderrättelseverksamheten och som finns i uppgiftssamlingar. Detta ska gälla även om uppgifterna omfattas av sekretess enligt 38 kap. 4 § offentlighets- och sekretesslagen (uppgifter om enskilds personliga och ekonomiska förhållanden).

Om det behövs för samarbetet mot terrorism eller vid svenskt deltagande i annat internationellt underrättelse- och säkerhetssamarbete får, i den utsträckning det följer av lag eller förordning eller om regeringen i ett enskilt fall beslutat om det, en utländsk underrättelse- eller säkerhetstjänst medges direktåtkomst till personuppgifter som behandlas i försvarsunderrättelseverksamheten och som finns i uppgiftssamlingar.

Regeringen kan meddela föreskrifter eller särskilt beslut om vilka som i andra fall får ha direktåtkomst till gemensamt tillgängliga uppgifter.

Regeringen, eller den myndighet som regeringen bestämmer, kan meddela

1. ytterligare föreskrifter eller beslut i enskilda fall om omfattningen av direktåtkomsten, och
2. föreskrifter om behörighet och säkerhet vid sådan åtkomst.

Skäl för utredningens förslag: 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 som ansvarar för uppgiftssamlingen i det enskilda fallet tar ställning till om informationen ska lämnas ut. Direktåtkomst innebär således att den myndighet som har sådan åtkomst fritt kan avgöra vilka uppgifter den vill ta del av med den begränsning som följer av offentlighets- och sekretesslagens bestämmelser. Om en myndighet har direktåtkomst till uppgifter får dessa därför anses utlämnade i och med att ett system för direktåtkomst upprättats. Det saknar betydelse om myndigheten faktiskt använder sig av en viss uppgift eller inte. Eftersom bestämmelser om direktåtkomst inte har någon sekretessbrytande verkan i sig, förutsätter direktåtkomst att de aktuella uppgifterna inte omfattas av sekretess eller att det finns en skyldighet enligt lag eller förordning att lämna ut de aktuella uppgifterna till den som får ha direktåtkomst.

Direktåtkomst för Säkerhetspolisen och Försvarets radioanstalt

Av 1 kap. 15 § första stycket FM-PuL framgår att Försvarsmakten får medge Säkerhetspolisen och Försvarets radioanstalt direktåtkomst till sådana uppgifter i en uppgiftssamling för försvarsunderrättelseverksamhet som behövs för att myndigheterna, inom ramen för myndighetsöverskridande samverkan, ska kunna göra bedömningar på strategisk nivå av terrorhotet mot Sverige och svenska intressen.

Denna samverkan mellan de tre myndigheterna sker vid Nationellt centrum för terrorhotbedömning (NCT).

Tillgången till sådana uppgifter ska enligt den bestämmelsen vara förbehållen de personer inom myndigheterna som på grund av sina arbetsuppgifter inom sådan samverkan behöver ha tillgång till uppgifterna. Enligt samma bestämmelse får regeringen meddela föreskrifter om vilka myndigheter som i andra fall får ha direktåtkomst till uppgiftssamlingar. Vidare får regeringen, eller den myndighet som regeringen bestämmer, meddela ytterligare föreskrifter eller beslut i enskilda fall om omfattningen av direktåtkomsten. Enligt bestämmelsen gäller möjligheten att meddela föreskrifter även föreskrifter om behörighet och säkerhet vid sådan åtkomst.

Enligt 1 kap. 15 a § FM-PuL har de berörda myndigheterna rätt att ta del av sådana uppgifter som avses i 15 § första stycket trots sekretess enligt 38 kap. 4 § offentlighets- och sekretesslagen. Sekretess gäller enligt den paragrafen hos Försvarsmakten i försvarsunderrättelseverksamheten och den militära 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 denne lider skada eller men.

I motiven till bestämmelserna i FM-PuL anförde regeringen att eftersom direktåtkomst innebär att den mottagande myndigheten fritt kan avgöra vilka uppgifter – inom ramen för den beviljade direktåtkomsten – den vill ta del av, blir uppgifterna att anse som utlämnade i och med att direktåtkomst medges. En myndighet kan därför inte tillåta en annan myndighet direktåtkomst till uppgifter, som vid en sekretessprövning, den senare myndigheten inte med säkerhet skulle ha rätt att ta del av. Eftersom de uppgifter som myndigheterna inom ramen för samarbetet mot terrorism har för avsikt att lämna ut till varandra genom direktåtkomst omfattas av sekretess behövde sekretessen enligt regeringen sekretessen således på förhand brytas.

Regeringen konstaterade att det för Försvarsmaktens del finns en bestämmelse om uppgiftsskyldighet i 2 § lagen om försvarsunderrättelseverksamhet. Där anges att underrättelser ska rapporteras till berörda myndigheter. Denna uppgiftsskyldighet omfattar enligt regeringen dock inte den typ av uppgifter som myndigheterna inom samarbetet har behov av att utbyta och som de skulle få tillgängliggöra genom direktåtkomst.

Efter en genomgång av skilda sekretessbestämmelser fann regeringen att bestämmelsen i 38 kap. 4 § offentlighets- och sekretesslagen om sekretess för uppgifter om enskildas personliga och ekonomiska för hållanden som har ett omvänt skaderekvisit borde brytas genom en bestämmelse om uppgiftsskyldighet. Utlämnande av uppgifter som rör enskildas personliga och ekonomiska förhållanden torde i den aktuella situationen nästan alltid vara till skada eller men för den enskilde (prop. 2017/18:36 s. 29 f.).

Som nyss nämnts avser bestämmelserna om direktåtkomst i 1 kap. 15 § första stycket FM-PuL sådana uppgifter som behövs för att Försvarsmakten, Försvarets radioanstalt och Säkerhetspolisen, inom ramen för myndighetsöverskridande samverkan, ska kunna göra bedömningar på strategisk nivå av terrorhotet mot Sverige och svenska intressen (NCT).

Försvarsmakten och Försvarets radioanstalt har även på andra områden ett nära samarbete med varandra när det gäller yttre militära hot mot landet, förutsättningar för svenskt deltagande i fredsfrämjande och humanitära insatser eller hot mot säkerheten för svenska intressen vid genomförande av sådana insatser, konflikter utomlands med konsekvenser för internationell säkerhet och främmande makts agerande eller avsikter av väsentlig betydelse för svensk utrikes-, säkerhets- och försvarspolitik.

Försvarets radioanstalt och Försvarsmakten samarbetar vidare med varandra och med Säkerhetspolisen när det gäller kartläggning av verksamhet som rör strategiska förhållanden avseende internationell terrorism och annan grov gränsöverskridande brottslighet som kan hota väsentliga nationella intressen, utveckling och spridning av massförstörelsevapen, krigsmateriel, och produkter som avses i lagen (2000:1064) om kontroll av produkter med dubbla användningsområden och av tekniskt bistånd, allvarliga yttre hot mot samhällets infrastruktur och främmande underrättelseverksamhet mot svenska intressen.

Detta samarbete har stor betydelse för Sveriges försvar och säkerhet, inte minst mot bakgrund av den säkerhetspolitiska utveckling som har ägt rum under de senast åren. Samarbetet leder till att myndigheterna delger varandra underrättelser. Några sekretesshinder föreligger normalt inte för sådan delgivning. Samarbetet ställer emellertid krav på att myndigheterna på ett arbetsbesparande sätt kan ta del även av andra uppgifter hos varandra som de behöver för

sin underrättelse- och säkerhetstjänst. Hos Försvarsmakten bör direktåtkomsten för Säkerhetspolisen och Försvarets radioanstalt avse personuppgifter som utgör bearbetningsunderlag och analysresultat inom försvarsunderrättelseverksamheten och som finns i uppgiftssamlingar.

En del av dessa uppgifter kan röra uppgifter om enskilds personliga och ekonomiska förhållanden och kan därför inte göras tillgängliga för direktåtkomst utan ett särskilt stöd i lag. Bestämmelsen bör därför uttryckligen ge ett stöd för att bryta sekretessen i 38 kap. 4 § offentlighets- och sekretesslagen.

Direktåtkomst i internationellt försvars- och säkerhetssamarbete

Utvecklingen i Sverige och i omvärlden skärper kraven på Sveriges förmåga att värna sin säkerhet. Detta gäller inte minst på området försvarsunderrättelse- och säkerhetstjänst, där internationell samverkan i många fall är helt nödvändig för att Försvarsmakten och Försvarets radioanstalt ska kunna lösa sina uppgifter på detta område.

Samarbete sker i flera fall genom att ses och utbyta information i mötesform och/eller genom elektroniskt utlämnande av meddelanden och rapporter. I de fall där samarbete sker med stora behov av skyndsamhet, samt i de fall där samarbete syftar till att gemensamt följa ett skeende, är det i vissa fall nödvändigt att inom ramen för samarbetet tillgängliggöra information genom direktåtkomst.

Behov av skyndsamhet kan exempelvis uppstå inför ett förmodat förestående terrordåd. Behov av att kunna medge direktåtkomst kan även uppstå på andra områden såsom när Försvarsmakten eller Försvarets radioanstalt följer ett underrättelsemässigt intressant skeende tillsammans med en internationell partner.

I sådana fall är det angeläget att kunna tillgängliggöra ett samlat kunskapsläge över tid, vilket lämpligen görs genom att Försvarsmakten medger en partner direktåtkomst till en uppgiftssamling som etablerats specifikt för detta samarbete.

För Försvarsmaktens del föreslås därför en bestämmelse som innebär att en utländsk underrättelse- eller säkerhetstjänst får medges direktåtkomst till personuppgifter som behandlas i försvarsunderrättelseverksamheten och som finns i uppgiftssamlingar. Som förutsättning bör gälla att det behövs för samarbetet mot terrorism

eller vid svenskt deltagande i annat internationellt underrättelse- och säkerhetssamarbete. Vidare bör det bara få ske i den utsträckning det följer av lag eller förordning eller om regeringen i ett enskilt fall beslutat om det.

Reglering i förordning

Utredningen anser att i den förordning som knyter an till lagen bör föras in ytterligare föreskrifter om direktåtkomst enligt vad som framgår av det följande och som till en del kommenteras.

Försvar och säkerhet

1. Försvarets materielverk får medges direktåtkomst till personuppgifter som behandlas med stöd av 2 kap. 1 § lagen (2019:000) om behandling av personuppgifter vid Försvarsmakten. Direktåtkomsten får endast avse personuppgifter som rör Försvarsmaktens materiel- och logistikförsörjning och som har gjorts gemensamt tillgängliga.

För Försvarets materielverk finns ett behov av direktåtkomst med anledning av uppdraget att materiel- och logistikförsörja Försvarsmakten. Dessa gemensamt tillgängliga uppgifter innehåller uppgifter om anställda vid Försvarsmakten och Försvarets materielverk samt uppgifter om personer hos leverantörer.

2. Totalförsvarets rekryteringsmyndighet får medges direktåtkomst till personuppgifter som behandlas med stöd av 2 kap. 1 § lagen (2019:000) om behandling av personuppgifter vid Försvarsmakten. Direktåtkomsten får endast avse personuppgifter som rör totalförsvarspliktiga och Försvarsmaktens krigsorganisation och som har gjorts gemensamt tillgängliga.

För Totalförsvarets rekryteringsmyndighet finns behovet med anledning av uppdraget avseende totalförsvarspliktiga. Försvarsmakten har direktåtkomst till system hos Totalförsvarets rekryteringsmyndighet.

3. Finlands försvarsmakt får medges direktåtkomst till personuppgifter som behandlas med stöd av 2 kap. 1 § lagen (2019:000) om behandling av

personuppgifter vid Försvarsmakten om det behövs för planering, förberedelser och genomförande av stöd inom ramen för lagen (2019:000) om operativt militärt stöd mellan Sverige och Finland. Direktåtkomsten får endast avse personuppgifter som har gjorts gemensamt tillgängliga.

I betänkandet SOU 2018:31 föreslås en lag om operativt militärt stöd mellan Sverige och Finland. I betänkandet föreslås vidare en förordning om utlämnande av sekretessbelagda uppgifter vid operativt stöd inom försvarssamarbetet mellan Sverige och Finland. Uppgift för vilken sekretess gäller enligt 15 kap. 2 § offentlighets- och sekretesslagen (2009:400) får enligt förslaget lämnas ut av Försvarsmakten, Försvarets materielverk och Totalförsvarets forskningsinstitut till en finsk myndighet avseende planering, förberedelser och genomförande av stöd inom ramen för den föreslagna lagen om operativt militärt stöd mellan Sverige och Finland. Bestämmelserna föreslås träda i kraft den 1 juli 2019. För ett effektivt planerings- och förberedelsearbete liksom för ett effektivt genomförande av samarbetet är finsk direktåtkomst till uppgifter hos Försvarsmakten viktig. Uppgifterna kan innehålla personuppgifter, bl.a. personal hos Försvarsmakten men framför allt om personer hos motståndare eller andra aktörer.

Försvarsunderrättelseverksamhet

1. Regeringskansliet, Säkerhetspolisen, Nationella operativa avdelningen i Polismyndigheten, Inspektionen för strategiska produkter, Försvarets materielverk, Totalförsvarets forskningsinstitut, Myndigheten för samhällsskydd och beredskap och Tullverket får medges direktåtkomst till personuppgifter som utgör analysresultat och underrättelser och som finns i uppgiftssamlingar för försvarsunderrättelseverksamhet.

En motsvarande bestämmelse finns för Försvarets radioanstalt i 9 § FRA-PuL och tas in i den förordning som ska knyta an till den föreslagna lagen om behandling av personuppgifter vid Försvarets radioanstalt.

2. Om det behövs för samarbetet mot terrorism eller vid svenskt deltagande i annat internationellt underrättelse- och säkerhetssamarbete

får en utländsk underrättelse- eller säkerhetstjänst medges direktåtkomst till personuppgifter som behandlas enligt 2 kap. 2 § lagen (2019:000) om behandling av personuppgifter vid Försvarsmakten och som finns i en uppgiftssamling som Försvarsmakten upprättat i syfte att dela informationen med mottagaren.

Innan direktåtkomst medges en utländsk underrättelse- eller säkerhetstjänst enligt första stycket ska Försvarsmakten underrätta Regeringskansliet (Försvarsdepartementet).

I Försvarsmaktens internationella samarbete med underrättelse- eller säkerhetstjänster i andra länder är finns ett behov av att kunna dela med sig information. Detta är särskilt påtagligt när det gäller samarbetet mot terrorism men gäller även övrigt samarbete. Enligt Försvarsmaktens bedömning kan man i framtiden etablera samarbeten som tekniskt skulle göra det möjligt att medge direktåtkomst hos Försvarsmakten. En sådan möjlighet gör samarbetet effektivare än annars, särskilt i brådskande situationer.

Militär säkerhetstjänst

1. Säkerhetspolisen, Nationella operativa avdelningen i Polismyndigheten, Myndigheten för samhällsskydd och beredskap, Migrationsverket, Försvarets materielverk, Försvarets radioanstalt, Totalförsvarets forskningsinstitut, Totalförsvarets rekryteringsmyndighet, Fortifikationsverket och Försvarshögskolan får medges direktåtkomst till personuppgifter som behandlas med stöd av 2 kap. 5 § första stycket 1 och 2 lagen (2019:000) om behandling av personuppgifter vid Försvarsmakten och som finns i en uppgiftssamling för säkerhetsunderrättelsetjänst.

Försvarsmakten har till uppgift enligt 39 § säkerhetsskyddsförordningen att kontrollera säkerhetsskyddet hos Fortifikationsverket, Försvarshögskolan, och de myndigheter som hör till Försvarsdepartementet. För dessa myndigheter, som är av särskild vikt för totalförsvaret, behöver Försvarsmakten få möjlighet att genom direktåtkomst tillgängliggöra personuppgifter, kopplade till misstänkt eller konstaterad säkerhetshotande verksamhet. Syftet med detta är dels att göra det möjligt för Försvarsmakten att sprida kunskap om säkerhetshotande aktörer till de samverkande myndigheter som

saknar egen inhämtning på säkerhetsunderrättelseområdet, dels att möjliggöra löpande informationsspridning under pågående säkerhetshotande verksamhet.

Att Försvarsmakten har möjlighet att tillgängliggöra denna information genom direktåtkomst innebär en väsentligt förbättrad möjlighet för att kritisk information kan delges samverkande myndigheter i tid.

För att Försvarsmakten ska kunna kartlägga verksamhet som utgör hot mot Sveriges säkerhet är myndigheten i flera fall beroende av samverkan med andra myndigheter. Detta gäller dels de myndigheter som bedriver egen uppföljning av säkerhetshotande verksamhet, såsom Polismyndigheten, Säkerhetspolisen och Myndigheten för samhällsskydd och beredskap. För uppföljning av sådan säkerhetshotande verksamhet som är gränsöverskridande är Försvarsmakten vidare beroende av samverkan med Tullverket och Migrationsverket. Samverkan med dessa myndigheter bedrivs redan genom möten, översändande av rapporter m.m. Genom att Försvarsmakten har möjlighet att tillgängliggöra denna information genom direktåtkomst ökar effektiviteten i samarbetet.

2. Säkerhetspolisen får medges direktåtkomst till personuppgifter som behandlas med stöd av 2 kap. 5 § första stycket 5 lag (2019:000) om behandling av personuppgifter vid Försvarsmakten och som finns i en uppgiftssamling för säkerhetsskyddstjänst.

Bestämmelsen motsvarar 9 § FM-PuF.

3. Om det behövs för samarbetet mot säkerhetshotande verksamhet som riktas mot Försvarsmakten och dess säkerhetsintressen får en utländsk underrättelse- eller säkerhetstjänst medges direktåtkomst till personuppgifter som behandlas med stöd av 2 kap. 5 § 1 och 2 och som finns i en avskild uppgiftssamling som Försvarsmakten upprättat i syfte att dela informationen med mottagaren. för säkerhetsunderrättelsetjänst.

Innan direktåtkomst medges en utländsk underrättelse- eller säkerhetstjänst ska Försvarsmakten underrätta Regeringskansliet (Försvarsdepartementet).

Liksom i försvarsunderrättelseverksamheten har Försvarsmakten i sin militära säkerhetstjänst ett behov av att kunna dela med sig information i samarbetet med underrättelse- eller säkerhetstjänster i andra länder.

Enligt Försvarsmaktens bedömning kan man i framtiden etablera samarbeten som tekniskt skulle göra det möjligt att medge direktåtkomst hos Försvarsmakten. En sådan möjlighet gör samarbetet effektivare än annars, särskilt i brådskande situationer.

Omfattning av direktåtkomst

Försvarsmakten beslutar om omfattningen av direktåtkomst som följer av lag, förordning eller regeringens beslut i enskilt fall.

Försvarsmakten ska säkerställa att förutsättningarna för direktåtkomsten dokumenteras.

Tillgången till uppgifter hos mottagaren ska vara förbehållen de personer som på grund av sina arbetsuppgifter behöver ha tillgång till uppgifterna.

Direktåtkomst får inte medges innan Försvarsmakten har försäkrat sig om att mottagaren uppfyller kraven på behörighet och säkerhet.

Utredningen föreslår till vissa delar ny reglering som möjliggör direktåtkomst hos Försvarsmakten under särskilt angivna premisser. I likhet med vad som följer av gällande regelverk är det Försvarsmakten som beslutar i vilken omfattning direktåtkomst bör medges. Den föreslagna bestämmelsen tydliggör detta. Bestämmelsen slår också fast att tillgången av uppgifter hos mottagaren ska vara förbehållen de personer som på grund av sina arbetsuppgifter behöver ha tillgång till uppgifterna, liksom att någon direktåtkomst inte kan medges innan dess att Försvarsmakten har försäkrat sig om att mottagaren uppfyller kraven på behörighet och säkerhet.

6.5.3 Direktåtkomst till personuppgifter hos Försvarets radioanstalt

Utredningens förslag: Säkerhetspolisen och Försvarsmakten får medges direktåtkomst till personuppgifter som utgör analysresultat inom försvarsunderrättelseverksamheten och som finns i uppgiftssamlingar. Detta ska gälla även om uppgifterna omfattas av sekretess enligt 38 kap. 4 § offentlighets- och sekretesslagen (uppgifter om enskilds personliga och ekonomiska förhållanden).

Om det behövs för samarbetet mot terrorism eller för annat internationellt säkerhetssamarbete får, i den utsträckning det följer av lag eller förordning eller om regeringen i ett enskilt fall beslutar om det, en utländsk underrättelse- eller säkerhetstjänst medges direktåtkomst till personuppgifter som behandlas i försvarsunderrättelseverksamheten och som finns i uppgiftssamlingar.

Om det behövs för samarbetet mot it-relaterade hot mot samhällsviktiga system får, i den utsträckning det följer av lag eller förordning eller om regeringen i ett enskilt fall beslutar om det, en utländsk organisation inom informationssäkerhetsområdet medges direktåtkomst till personuppgifter som behandlas i informationssäkerhetsverksamheten och som finns i uppgiftssamlingar.

Regeringen kan meddela föreskrifter eller särskilt beslut om vilka som i andra fall får ha direktåtkomst till gemensamt tillgängliga uppgifter.

Regeringen, eller den myndighet som regeringen bestämmer, kan meddela

1. ytterligare föreskrifter eller beslut i enskilda fall om omfattningen av direktåtkomsten, och
2. föreskrifter om behörighet och säkerhet vid sådan åtkomst.

Skäl för förslaget: Vad direktåtkomst innebär beskrivs i föregående avsnitt 6.5.2.

Direktåtkomst för Säkerhetspolisen och Försvarsmakten

Av 1 kap. 15 § första stycket FRA-PuL framgår att Försvarets radioanstalt får medge Säkerhetspolisen och Försvarsmakten direktåtkomst till sådana uppgifter i en uppgiftssamling för försvarsunderrättelseverksamhet som behövs för att myndigheterna, inom ramen för myndighetsöverskridande samverkan, ska kunna göra bedömningar på strategisk nivå av terrorhotet mot Sverige och svenska intressen. Denna samverkan mellan de tre myndigheterna sker vid Nationellt centrum för terrorhotbedömning (NCT).

Tillgången till sådana uppgifter ska enligt denna bestämmelse vara förbehållen de personer inom myndigheterna som på grund av sina arbetsuppgifter inom sådan samverkan behöver ha tillgång till uppgifterna. Enligt samma bestämmelser får regeringen meddela föreskrifter om vilka myndigheter som i andra fall får ha direktåtkomst till uppgiftssamlingar. Vidare får regeringen, eller den myndighet som regeringen bestämmer, meddela ytterligare föreskrifter eller beslut i enskilda fall om omfattningen av direktåtkomsten. Enligt bestämmelsen gäller möjligheten att meddela föreskrifter även föreskrifter om behörighet och säkerhet vid sådan åtkomst.

Enligt 1 kap. 15 a § FRA-PuL har de berörda myndigheterna rätt att ta del av sådana uppgifter som avses i 15 § första stycket trots sekretess enligt 38 kap. 4 § offentlighets- och sekretesslagen. Sekretess gäller enligt den paragrafen hos Försvarets radioanstalt i försvarsunderrättelse- och utvecklingsverksamheten 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 denne lider skada eller men.

I motiven till bestämmelserna i FRA-PuL anförde regeringen att eftersom direktåtkomst innebär att den mottagande myndigheten fritt kan avgöra vilka uppgifter – inom ramen för den beviljade direktåtkomsten – den vill ta del av, blir uppgifterna att anse som utlämnade i och med att direktåtkomst medges. En myndighet kan därför inte tillåta en annan myndighet direktåtkomst till uppgifter, som vid en sekretessprövning, den senare myndigheten inte med säkerhet skulle ha rätt att ta del av. Eftersom de uppgifter som myndigheterna inom ramen för samarbetet mot terrorism har för avsikt att lämna ut till varandra genom direktåtkomst omfattas av sekretess

behövde sekretessen enligt regeringen sekretessen således på förhand brytas.

Regeringen konstaterade att för Försvarets radioanstalts del finns en bestämmelse om uppgiftsskyldighet i 2 § lagen om försvarsunderrättelseverksamhet. Där anges att underrättelser ska rapporteras till berörda myndigheter. Denna uppgiftsskyldighet omfattar enligt regeringen dock inte den typ av uppgifter som myndigheterna inom samarbetet har behov av att utbyta och som de skulle få tillgängliggöra genom direktåtkomst.

Efter en genomgång av skilda sekretessbestämmelser fann regeringen att bestämmelsen i 38 kap. 4 § offentlighets- och sekretesslagen om sekretess för uppgifter om enskildas personliga och ekonomiska för hållanden som har ett omvänt skaderekvisit borde brytas genom en bestämmelse om uppgiftsskyldighet. Utlämnande av uppgifter som rör enskildas personliga och ekonomiska förhållanden torde i den aktuella situationen nästan alltid vara till skada eller men för den enskilde (prop. 2017/18:36 s. 29 f.).

Som nyss nämnts avser bestämmelserna om direktåtkomst i 1 kap. 15 § första stycket FRA-PuL sådana uppgifter som behövs för att Försvarsmakten, Försvarets radioanstalt och Säkerhetspolisen, inom ramen för myndighetsöverskridande samverkan, ska kunna göra bedömningar på strategisk nivå av terrorhotet mot Sverige och svenska intressen (NCT).

Försvarets radioanstalt och Försvarsmakten har även på andra områden ett nära samarbete med varandra när det gäller yttre militära hot mot landet, förutsättningar för svenskt deltagande i fredsfrämjande och humanitära insatser eller hot mot säkerheten för svenska intressen vid genomförande av sådana insatser, konflikter utomlands med konsekvenser för internationell säkerhet och främmande makts agerande eller avsikter av väsentlig betydelse för svensk utrikes-, säkerhets- och försvarspolitik.

Försvarets radioanstalt och Försvarsmakten samarbetar vidare med varandra och med Säkerhetspolisen när det gäller kartläggning av verksamhet som rör strategiska förhållanden avseende internationell terrorism och annan grov gränsöverskridande brottslighet som kan hota väsentliga nationella intressen, utveckling och spridning av massförstörelsevapen, krigsmateriel, och produkter som avses i lagen om kontroll av produkter med dubbla användningsområden och av tekniskt bistånd, allvarliga yttre hot mot samhällets

infrastruktur och främmande underrättelseverksamhet mot svenska intressen.

Detta samarbete har stor betydelse för Sveriges försvar och säkerhet, inte minst mot bakgrund av den säkerhetspolitiska utveckling som har ägt rum under de senast åren. Samarbetet leder till att myndigheterna delger varandra underrättelser. Några sekretesshinder föreligger normalt inte för sådan delgivning. Samarbetet ställer emellertid krav på att myndigheterna på ett arbetsbesparande sätt kan ta del även av andra uppgifter hos varandra som de behöver för sin underrättelse- och säkerhetstjänst. Hos Försvarets radioanstalt bör direktåtkomsten för Säkerhetspolisen och Försvarsmakten avse personuppgifter som utgör analysresultat och som finns i uppgiftssamlingar.

En del av dessa uppgifter kan röra uppgifter om enskilds personliga och ekonomiska förhållanden och kan därför inte göras tillgängliga för direktåtkomst utan ett särskilt stöd i lag. Bestämmelsen bör därför uttryckligen ge ett stöd för att bryta sekretessen i 38 kap. 4 § offentlighets- och sekretesslagen.

Direktåtkomst i internationellt försvarsunderrättelsesamarbete

Utvecklingen i Sverige och i omvärlden skärper kraven på Sveriges förmåga att värna sin säkerhet. Detta gäller inte minst försvarsunderrättelseverksamheten där internationell samverkan i många fall är helt nödvändigt för att Försvarets radioanstalt ska kunna lösa sina uppgifter på detta område.

Samarbete sker i flera fall genom att utbyta information i mötesform eller genom elektroniskt utlämnande av meddelanden och rapporter. I de fall där samarbete sker med stora behov av skyndsamhet, samt i de fall där samarbete syftar till att gemensamt följa ett skeende, är det i vissa fall nödvändigt att inom ramen för samarbetet tillgängliggöra information genom direktåtkomst.

Behov av skyndsamhet kan exempelvis uppstå inför ett förmodat förestående terrordåd. Behov av att kunna medge direktåtkomst kan även uppstå på andra områden såsom när eller Försvarets radioanstalt följer ett underrättelsemässigt intressant skeende tillsammans med en internationell partner.

I sådana fall är det angeläget att kunna tillgängliggöra ett samlat kunskapsläge över tid, vilket lämpligen görs genom att Försvarets

radioanstalt medger en partner direktåtkomst till personuppgifter som finns i uppgiftssamlingar.

För Försvarets radioanstalt föreslås därför en bestämmelse som innebär att en utländsk underrättelse- eller säkerhetstjänst får medges direktåtkomst till personuppgifter som behandlas i försvarsunderrättelseverksamheten och som finns i uppgiftssamlingar. Som förutsättning bör gälla att det behövs för samarbetet mot terrorism eller för annat internationellt säkerhetssamarbete. Vidare bör det bara få ske i den utsträckning det följer av lag eller förordning eller om regeringen i ett enskilt fall beslutat om det.

Direktåtkomst i internationellt informationssäkerhetssamarbete

Utvecklingen på informationssäkerhetsområde präglas av omfattande it-attacker och andra typer av intrång i viktiga informationssystem. Företeelsen är global och kräver internationellt samarbete mellan organisationer som verkar på informationssäkerhetsområdet. Kännetecknande för samarbetet är att det ofta ställer krav på snabbt tillgänglig information för att man ska kunna vidta lämpliga åtgärder för att förhindra eller minimera skadeverkningar. Mot denna bakgrund föreslår utredningen att det ska vara möjligt för Försvarets radioanstalt att medge en utländsk organisation inom informationssäkerhetsområdet direktåtkomst till personuppgifter som behandlas i informationssäkerhetsverksamheten och som finns i uppgiftssamlingar. Som förutsättning bör gälla att det behövs för samarbetet mot it-relaterade hot mot samhällsviktiga system. Vidare bör det även i detta fall bara få ske i den utsträckning det följer av lag eller förordning eller om regeringen i ett enskilt fall beslutat om det.

Reglering i förordning

Utredningen anser att i den förordning som knyter an till lagen bör föras in ytterligare föreskrifter om direktåtkomst enligt vad som framgår av det följande och som till en del kommenteras.

Försvarsunderrättelseverksamhet

Regeringskansliet, Säkerhetspolisen, Nationella operativa avdelningen i Polismyndigheten, Inspektionen för strategiska produkter, Försvarsmakten, Försvarets materielverk, Totalförsvarets forskningsinstitut, Myndigheten för samhällsskydd och beredskap och Tullverket får medges direktåtkomst till personuppgifter som utgör underrättelser och som finns i uppgiftssamlingar.

Bestämmelsen motsvarar 9 § FRA-PuL.

Informationssäkerhetsverksamhet

Säkerhetspolisen och Försvarsmakten får medges direktåtkomst till personuppgifter som utgör analysresultat och som behandlas i en uppgiftssamling för informationssäkerhetsverksamhet.

Utvecklingen på informationssäkerhetsområdet med ett ökande antal skadliga intrång i för samhället viktiga och känsliga informationssystem kräver ett nära samarbete mellan Försvarets radioanstalt, Försvarsmakten och Säkerhetspolisen. Möjligheterna för Säkerhetspolisen och Försvarsmakten att få direktåtkomst till personuppgifter som utgör analysresultat hos Försvarets radioanstalt medför att samarbetet blir effektivare och att skyddet för de mest skyddsvärda informationssystemen kan stärkas.

Övrigt

Försvarets radioanstalt beslutar om omfattningen av direktåtkomst som följer av lag, förordning eller regeringens beslut i enskilt fall.

Försvarets radioanstalt ska säkerställa att förutsättningarna för direktåtkomsten dokumenteras.

Tillgången till uppgifter ska vara förbehållen de personer som på grund av sina arbetsuppgifter behöver ha tillgång till uppgifterna.

Direktåtkomst får inte medges innan Försvarets radioanstalt har försäkrat sig om att den mottagande parten uppfyller kraven på behörighet och säkerhet.

Utredningen föreslår till vissa delar ny reglering som möjliggör direktåtkomst hos Försvarets radioanstalt under särskilt angivna premisser. I likhet med vad som följer av gällande bestämmelser är det Försvarets radioanstalt som beslutar i vilken omfattning direktåtkomst bör medges. Den föreslagna bestämmelsen tydliggör detta. Bestämmelsen slår också fast att tillgången av uppgifter hos mottagaren ska vara förbehållen de personer som på grund av sina arbetsuppgifter behöver ha tillgång till uppgifterna, liksom att någon direktåtkomst inte kan medges innan dess att Försvarets radioanstalt har försäkrat sig om att mottagaren uppfyller kraven på behörighet och säkerhet.

6.6 Skyldigheter som personuppgiftsansvarig

6.6.1 Författningsenlig behandling genom lämpliga tekniska och organisatoriska åtgärder

Utredningens förslag: Försvarsmakten och Försvarets radioanstalt ska genom lämpliga tekniska och organisatoriska åtgärder säkerställa att behandlingen av personuppgifter är författningsenlig och skydda rättigheterna för dem som uppgifterna rör.

Skäl för utredningens förslag: Någon bestämmelse om att Försvarsmakten och Försvarets radioanstalt genom lämpliga tekniska och organisatoriska åtgärder ska säkerställa att behandlingen av personuppgifter är författningsenlig och att den enskildes rättigheter skyddas finns inte i FM-PuL eller FRA-PuL.

Förslaget till Säkerhetspolisens datalag innehåller bestämmelser om personuppgiftsansvarigas skyldigheter, däribland att vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen av personuppgifter är författningsenlig och att registrerades rättigheter skyddas. Lämpliga tekniska och organisatoriska åtgärder ska enligt dessa bestämmelser vidtas med beaktande av behandlingens art, omfattning, sammanhang och ändamål och riskerna för fysiska personers rättigheter och friheter (SOU 2017:74).

I de föreslagna lagarna bör enligt utredningen införas en generell skyldighet för Försvarsmakten och Försvarets radioanstalt, att genom lämpliga tekniska och organisatoriska åtgärder säkerställa att

behandlingen av personuppgifter är författningsenlig och att myndigheterna skyddar rättigheterna för den vars uppgifter behandlas. Det är däremot inte möjligt att i de föreslagna lagarna närmare ange vilka tekniska och organisatoriska åtgärder som Försvarsmakten och Försvarets radioanstalt bör vidta, utan detta får avgöras beroende på vilken verksamhet hos de båda myndigheterna det rör sig om.

Utredningen anser att ett krav på att Försvarsmakten och Försvarets radioanstalt inte bara ska säkerställa att behandlingen utförs författningsenligt utan också ska *kunna visa* att så är fallet går för långt och skulle innebära betungande rutiner. Den tillsyn och kontroll som ska ske är en tillräcklig funktion.

Vilka omständigheter som Försvarsmakten och Försvarets radioanstalt ska beakta vid beslut om åtgärder enligt de föreslagna bestämmelserna bör regleras i de förordningar som ska knyta an till lagarna. Där bör anges att de tekniska och organisatoriska åtgärder som Försvarsmakten och Försvarets radioanstalt ska vidta ska vara rimliga med beaktande av behandlingens art, omfattning, sammanhang och ändamål och de särskilda riskerna med behandlingen.

6.6.2 Myndigheterna ska föra loggar över personuppgiftsbehandling

Utredningens förslag: Försvarsmakten och Försvarets radioanstalt ska säkerställa att det i uppgiftsamlingar förs loggar över personuppgiftsbehandling.

Regeringen eller den myndighet regeringen bestämmer kan meddela föreskrifter om loggar.

Skäl för utredningens förslag: Som framgår av avsnitt 6.6.4 ska myndigheterna enligt 3 kap. 2 § första stycket FM-PuL och FRA-PuL vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Ett led i att vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas är loggning och logguppföljning. Därigenom säkerställs att bestämmelser som ska skydda den personliga integriteten tillämpas korrekt. Ett grundläggande säkerhetskrav är att genom loggar skapa en sådan spårbarhet att man kan upptäcka otillåten tillgång till personuppgifter eller om det sker otillåtna sökningar.

Loggarna ska följas upp regelbundet och för att skapa en förebyggande effekt ska användarna informeras om att loggning och logguppföljning sker.

Varken i FM-PuL eller FRA-PuL finns någon uttrycklig bestämmelse om loggning. Utredningen anser att en sådan bestämmelse för tydlighetens skull bör införas i de nya lagarna. Enligt den bör Försvarsmakten och Försvarets radioanstalt säkerställa att det förs loggar över personuppgiftsbehandling av gemensamt tillgängliga uppgifter i den utsträckning regeringen eller den myndighet regeringen bestämmer föreskriver.

I de förordningar som ska knyta an till lagarna bör tas in föreskrifter om loggar.

För Försvarsmaktens del bör där anges att skyldigheten att föra loggar gäller myndighetens informationssystem som innehåller gemensamt tillgängliga uppgifter.

För Försvarets radioanstalts del bör där anges att Försvarets radioanstalt ska föra loggar i myndighetens informationssystem som innehåller uppgiftssamlingar för försvarsunderrättelse- och informationssäkerhetsverksamhet. I båda fallen ska det av loggarna framgå vilken medarbetare eller annan som läst, skapat, ändrat eller raderat personuppgifter, samt tidpunkten för åtgärden. I båda fallen ska skyldigheten att föra loggar inte gälla informationssystem som ännu inte börjat användas.

6.6.3 Myndigheterna ska begränsa tillgången till personuppgifter

Utredningens förslag: I de föreslagna lagarna ska föras in en föreskrift om att tillgången till personuppgifter ska alltid begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter.

Skäl för utredningens förslag: Av 1 kap. 16 § FM-PuL och FRA-PuL framgår att tillgången till personuppgifter alltid ska begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter. Motiven finns i prop. 2006/07:46 s. 96. Utredningen anser att en motsvarande bestämmelse ska föras in i de nya lagarna.

6.6.4 Säkerheten för personuppgifter

Utredningens förslag: I de föreslagna lagarna ska föras in en föreskrift om att Försvarsmakten respektive Försvarets radioanstalt ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas, särskilt mot obehörig eller otillåten behandling eller förstöring och mot förlust eller annan oavsiktlig skada.

Skäl för utredningens förslag: Av 3 kap. 2 § FM-PuL och FRA-PuL framgår att Försvarsmakten respektive Försvarets radioanstalt ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna ska 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. Motiven till bestämmelsen finns i prop. 2006/07:46 s. 95 f. Utredningen anser att en motsvarande bestämmelse bör införas i de nya lagarna.

6.6.5 Dataskyddsombud

Utredningens förslag: Försvarsmakten och Försvarets radioanstalt ska utse ett eller flera dataskyddsombud och anmäla till tillsynsmyndigheten när dataskyddsombud utses och entledigas.

Dataskyddsombudet ska

1. självständigt kontrollera att myndigheten behandlar personuppgifter författningsenligt och på ett korrekt sätt och i övrigt fullgör sina skyldigheter,
2. informera och ge råd till myndigheten och till dem som behandlar personuppgifter under myndighetens ledning om deras skyldigheter vid behandling av personuppgifter,
3. samråda med tillsynsmyndigheten, och

4. föra en förteckning över de kategorier av behandlingar som myndigheten ansvarar för och som är helt eller delvis automatiserade.

Regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter om vad en förteckning som avses i 4 ska innehålla.

Om Försvarsmakten eller Försvarets radioanstalt bryter mot de bestämmelser som gäller för behandlingen av personuppgifter och rättelse inte vidtas, ska dataskyddsombudet anmäla det till tillsynsmyndigheten.

Skäl för utredningens förslag: Enligt 4 kap. 1 § FM-PuL och FRA-PuL ska Försvarsmakten och Försvarets radioanstalt utse ett eller flera personuppgiftsombud och anmäla dessa till tillsynsmyndigheten.

Personuppgiftsombudet har 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,
- anmäla till tillsynsmyndigheten om personuppgiftsombudet har anledning att misstänka att Försvarsmakten respektive Försvarets radioanstalt bryter mot de bestämmelser som gäller för behandlingen av personuppgifter och inte vidtar rättelse så snart det kan ske efter påpekande,
- även i övrigt samråda med tillsynsmyndigheten vid tveksamhet om hur de bestämmelser som gäller för behandlingen av personuppgifter ska tillämpas,
- föra en förteckning över de behandlingar som Försvarsmakten respektive Försvarets radioanstalt genomför och som är helt eller delvis automatiserade och
- hjälpa registrerade att få rättelse när det finns anledning att misstänka att behandlade personuppgifter är felaktiga eller ofullständiga.

Motiven finns i prop. 2006/07:46 s. 98.

I den lagstiftning om behandling av personuppgifter som helt eller delvis bygger på unionsrätten har benämningen personuppgiftsombud ersatts av benämningen dataskyddsombud. Unionsrätten är som tidigare anförts inte tillämplig på den behandling av personuppgifter som omfattas av de lagförslag som utredningen lägger fram och utredningen anser inte att samma regler som gäller för dataskyddsombud enligt dataskyddsförordningen bör gälla på detta område. Dock finner utredningen att det är lämpligt att använda benämningen dataskyddsombud i stället för personuppgiftsombud i de lagförslag som utredningen lägger fram.

Dataskyddsombudet bör ha samma uppgifter som personuppgiftsombudet har enligt FM-PuL och FRA-PuL, med undantag av skyldigheten att hjälpa registrerade att få rättelse när det finns anledning att misstänka att behandlade personuppgifter är felaktiga eller ofullständiga. Den uppgiften bör ligga på den personuppgiftsansvarige.

6.6.6 Personuppgiftsbiträden

Utredningens förslag: Försvarsmakten respektive Försvarets radioanstalt får, om det är lämpligt, anlita personuppgiftsbiträden för behandling av personuppgifter på Försvarsmaktens respektive Försvarets radioanstalts vägnar. Innan ett personuppgiftsbiträde anlitas, ska myndigheten försäkra sig om att biträdet kommer att vidta de lämpliga tekniska och organisatoriska åtgärder som krävs för att behandlingen av personuppgifter ska vara författningsenlig och för att skydda rättigheterna för den som uppgifterna rör.

Personuppgiftsbiträdets behandling av personuppgifter ska regleras i ett skriftligt avtal eller annan skriftlig överenskommelse.

Ett personuppgiftsbiträde får inte anlita ett annat personuppgiftsbiträde utan skriftligt tillstånd av myndigheten.

Ett personuppgiftsbiträde eller den eller de personer som arbetar under biträdets eller myndighetens ledning ska behandla personuppgifter i enlighet med instruktioner från myndigheten.

Om ett personuppgiftsbiträde, i strid med myndighetens instruktioner, bestämmer ändamålen med och medlen för behandlingen, ska biträdet anses vara personuppgiftsansvarig enligt den föreslagna lagen för den behandlingen.

Skyldigheten att säkerställa att det förs loggar ska också gälla för personuppgiftsbiträdet. Detsamma gäller kravet på att tillgången till personuppgifter sak begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter.

Personuppgiftsbiträdet ska också vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas, särskilt mot obehörig eller otillåtenbehandling eller förstöring och mot förlust eller annan oavsiktlig skada.

Skäl för utredningens förslag: Enligt 3 kap. 1 § FM-PuL och FRA-PuL får ett personuppgiftsbiträde och den eller de personer som arbetar under biträdet eller respektive myndighets ledning behandla personuppgifter bara i enlighet med instruktioner från myndigheten. Det ska enligt bestämmelsen finnas ett skriftligt avtal om personuppgiftsbiträdets behandling av personuppgifter för myndighetens räkning. I det avtalet ska särskilt anges att personuppgiftsombudet får behandla personuppgifterna bara i enlighet med instruktioner från myndigheten och att personuppgiftsbiträdet är skyldigt att vidta lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifter som behandlas.

När myndigheten anlitar ett personuppgiftsbiträde ska den enligt 3 kap. 2 § FM-PuL och FRA-PuL förvissa sig om att ett personuppgiftsbiträde kan genomföra de säkerhetsåtgärder som måste vidtas och se till att personuppgiftsbiträdet verkligen vidtar åtgärderna.

Motiven till bestämmelserna finns i prop. 2006/07:46 s. 95.

Utredningen anser att motsvarande reglering bör införas i de nya lagarna. Följande föreskrifter bör dock läggas till.

Ett personuppgiftsbiträde får inte anlita ett annat personuppgiftsbiträde utan skriftligt tillstånd från myndigheten.

Om ett personuppgiftsbiträde, i strid med myndighetens instruktioner, bestämmer ändamålen med och medlen för behandlingen, ska personuppgiftsbiträdet vara personuppgiftsansvarig enligt den föreslagna lagen för den behandlingen.

Skyldigheten att säkerställa att det förs loggar ska också gälla för personuppgiftsbiträdet. Detsamma gäller kravet på att tillgången till personuppgifter sak begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter.

Personuppgiftsbiträdet ska också vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas, särskilt mot obehörig eller otillåten behandling eller förstöring och mot förlust eller annan oavsiktlig skada.

6.6.7 Bestämmelser om konsekvensbedömningar bör inte införas

Utredningens bedömning: Särskilda regler om konsekvensbedömningar bör inte införas i de föreslagna lagarna.

Skäl för utredningens bedömning: Enligt förslaget till Säkerhetspolisens datalag ska Säkerhetspolisen bedöma konsekvenserna för skyddet av personuppgifter om en typ av ny behandling, eller betydande förändringar avseende redan pågående behandling, kan antas medföra särskild risk för intrång i registrerades personliga integritet. Bedömningen ska ske innan typen av behandling påbörjas eller förändringen genomförs.

Om konsekvensbedömningen visar att det finns särskild risk för intrång i registrerades personliga integritet eller om typen av behandling innebär särskild risk för intrång, ska Säkerhetspolisen samråda med tillsynsmyndigheten i god tid innan behandlingen påbörjas eller betydande förändringar genomförs (5 kap. 6 § förslaget till Säkerhetspolisens datalag).

Reglerna om konsekvensbedömningar och skyldighet att samråda med tillsynsmyndigheten grundar sig på unionsrätten. I sammanhanget vill utredningen peka på skäl 93 i dataskyddsförordningen om konsekvensbedömningar. Där sägs att medlemsstaterna kan anse det nödvändigt att genomföra en sådan bedömning i samband med antagande av medlemsstaters nationella rätt som ligger till grund för utövande av myndighetens eller det offentliga organets uppgifter och reglerar den aktuella specifika behandlingsåtgärden eller serien av åtgärder. Den lagstiftning som utredningen föreslår består till en icke ringa del av bedömningar av konsekvenserna för skyddet av personuppgifter. Utredningen konstaterar att unionsrätten inte gäller de behandlingar av personuppgifter vid Försvarsmakten och Försvarets radioanstalt som utredningens lagförslag omfattar. Utredningen anser

att det inte heller finns några skäl att föreslå att det i lagförslagen förs in bestämmelser om konsekvensbedömningar.

6.7 Enskildas rättigheter

6.7.1 Allmän information som ska göras tillgänglig

Utredningens förslag: Försvarsmakten och Försvarets radioanstalt ska göra följande allmänna information tillgänglig:

1. Myndighetens identitet och kontaktuppgifter.
2. Uppgifter om dataskyddsombudet.
3. Ändamålen med behandlingen.
4. Rätten att begära att få information om behandling av personuppgifter och att få del av dem.
5. Rätten att begära rättelse, radering eller begränsning av behandlingen.

Skäl för utredningens förslag: Några regler om att myndigheterna ska hålla information allmänt tillgänglig finns inte i FM-PuL och FRA-PuL. Utredningen föreslår att viss information om Försvarsmakten och Försvarets radioanstalt ska vara allmänt tillgänglig. Med allmän menas information som riktar sig till en obestämd krets av personer. I kravet på att information ska vara tillgänglig ligger att allmänheten i princip ska ha möjlighet att ta del av informationen när den önskar. Informationen kan t.ex. publiceras på myndigheternas webbplatser eller finnas i en broschyr eller annan informationsskrift.

Utöver uppgifter om myndighetens identitet och kontaktuppgifter föreslås i det följande att viss annan allmän information på områden som har anknytning till personuppgiftsbehandling ska göras allmänt tillgänglig av myndigheterna.

Uppgifter om dataskyddsombudet

Dataskyddsombud behandlas i avsnitt 6.6.5.

I likhet med vad som föreslås i Säkerhetspolisens datalag anser utredningen att det finns skäl att i lag ha föreskrifter om att hålla vissa uppgifter om dataskyddsombudet allmänt tillgängliga. Det finns emellertid inte skäl att införa krav på att dataskyddsombudets identitet eller direkta kontaktuppgifter, exempelvis hans eller hennes e-postadress, ska göras allmänt tillgängliga, utan det är tillräckligt att det framgår att det finns ett dataskyddsombud och hur allmänheten kan kontakta honom eller henne.

Ändamålen med behandlingen

Den information som åsyftas i den föreslagna bestämmelsen avser, liksom de bestämmelser regeringen har föreslagit i brottsdatalagen (prop. 2017/18:232), att det är fråga om upplysningar av generell karaktär som gäller myndighetens personuppgiftsbehandling i allmänhet. Det innebär att det inte är fråga om ändamålen för behandling i varje enskilt fall som avses utan för vilka kategorier av ändamål personuppgifter får behandlas. Det bör emellertid inte krävas en uttömmande uppräkning av för vilka ändamål personuppgifter behandlas, utan det bör vara tillräckligt att enskilda genom informationen får en god bild av den personuppgiftsbehandling som Försvarsmakten eller Försvarets radioanstalt utför.

Information om vissa rättigheter

Som angetts ovan ska Försvarsmakten respektive Försvarets radioanstalt vidta vissa åtgärder efter begäran av en enskild. Någon bestämmelse om att information om dessa rättigheter ska göra allmänt tillgänglig finns inte i FM-PuL och FRA-PuL.

Utredningen anser att informationen också ska avse rätten att få information om behandling av personuppgifter och att få del av dem liksom rätten att begära rättelse, radering eller begränsning av behandlingen.

6.7.2 Enskilds rätt till personrelaterad information hos Försvarsmakten

Utredningens förslag:

Information som ska lämnas om uppgifterna samlas in från personen själv.
Om uppgifter om en person samlas in från personen själv, ska Försvarsmakten när personuppgifterna erhålls, självmant lämna följande information till den som uppgifterna rör:

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 som uppgifterna rör ska 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 som ska lämnas efter begäran
Försvarsmakten ska till den som begär det utan onödigt dröjsmål lämna skriftligt besked om personuppgifter som rör honom eller henne behandlas. Behandlas sådana uppgifter ska sökanden få del av dem och få följande skriftliga information.

1. Vilka personuppgifter om sökanden som behandlas.
2. Varifrån personuppgifterna kommer.
3. Den rättsliga grunden för behandlingen.
4. Ändamålen med behandlingen.
5. Mottagare eller kategorier av mottagare av personuppgifterna, även i annat land eller internationella organisationer.
6. Hur länge personuppgifterna får behandlas eller, om det inte är möjligt att ange, kriterierna för att fastställa det.
7. Rätten att begära rättelse, radering eller begränsning av behandlingen.

Sådant utlämnande behöver inte omfatta personuppgifter som sökanden har tagit del av, om inte han eller hon begär det. Det ska dock framgå av informationen att personuppgifterna i fråga behandlas.

Ansökan ska göras skriftligen hos Försvarsmakten och vara undertecknad av den sökande själv. Information enligt första stycket ska 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.

Skäl för utredningens förslag: Bestämmelser om att lämna information finns i 2 kap. 1 och 2 §§ FM-PuL.

Information som ska lämnas om uppgifterna samlas in från den som uppgifterna rör

Om uppgifter om en person samlas in i den militära säkerhetstjänsten från den som personuppgifterna rör ska Försvarsmakten i samband med insamlingen självmant lämna den registrerade information om behandlingen av uppgifterna. Sådan information ska omfatta uppgift om att det är Försvarsmakten som är personuppgiftsansvarig för behandlingen, uppgift om ändamålen med behandlingen och all övrig information som behövs för att den registrerade ska 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 (2 kap. 1 § FM-PuL). Av samma bestämmelse framgår att information inte behöver lämnas om sådant som den registrerade redan känner till.

Motiven finns i prop. 2006/07:46 s. 86 f. Bestämmelsen tillämpas huvudsakligen i samband med säkerhetsprövning enligt säkerhetsskyddslagen inför bl.a. anställning, uppdrag och tjänstgöring inom Försvarsmakten.

Information behöver inte lämnas om sådant som den personuppgifterna rör redan känner till. Sådant som denne redan känner till kan vara sådant som han eller hon vet t.ex. på grund av att informationen redan har lämnats i enlighet med annan lagstiftning eller när den personuppgiftsansvarige avser att fortlöpande samla in uppgifter om den uppgifterna rör. Information behöver då inte lämnas varje

gång nya uppgifter samlas in, om den uppgifterna rör en gång har fått fullständig information och således redan känner till informationen.

Liksom vid personuppgiftsbehandling inom ramen för den militära säkerhetstjänstens verksamhet förekommer situationer även inom andra av Försvarsmaktens verksamhetsområden där uppgifter inhämtas från den som personuppgifterna rör. Utredningen föreslår inte någon förändring beträffande den informationsskyldighet som enligt nuvarande bestämmelser omfattar verksamhet inom den militära säkerhetstjänsten. Som framgått i tidigare avsnitt föreslår emellertid utredningen att den nya lagen om personuppgiftsbehandling inom Försvarsmakten ska ha ett utvidgat tillämpningsområde. Även inom verksamhetsområdena *Sveriges försvar och säkerhet* samt *internationellt säkerhets- och försvarssamarbete* kan det förekomma situationer när Försvarsmakten behandlar personuppgifter som har lämnats av den enskilde själv. Det är därför inte lämpligt med lagens utvidgade tillämpningsområde att Försvarsmaktens informationsskyldighet begränsas till sådant som inhämtats inom ramen för den militära säkerhetstjänsten, utan Försvarsmakten bör även åläggas att lämna information om personuppgiftsbehandlingen som sker inom dessa tillkommande områden, dvs. Sveriges försvar och säkerhet samt internationellt säkerhets- och försvarssamarbete, när uppgifterna hämtas från den enskilde själv.

Information som ska lämnas efter begäran

Enligt 2 kap. 2 § FM-PuL är Försvarsmakten skyldig att till var och en som ansöker om det en gång per kalenderår gratis lämna besked om huruvida personuppgifter som rör den sökande behandlas eller inte (ärenden om personrelaterad information). En sökandes rätt enligt bestämmelserna att få reda på om personuppgifter som rör honom eller henne behandlas av Försvarsmakten gäller inte i den utsträckning som sekretess hindrar att uppgifterna lämnas ut till den registrerade, vilket framgår av 2 kap. 4 § FM-PuL. I motiven till bestämmelsen (prop. 2006/07:46 s. 89) anges att den sekretess som gäller för Försvarsmaktens verksamheter inom de områden som regleras av FM-PuL innebär att information sällan kommer lämnas

ut, men att bestämmelser om information fyller en viktig funktion i de fall där sekretess inte gäller för uppgifterna.

Sekretessbestämmelser som begränsar den enskildes rätt till insyn gäller emellertid inte i förhållande till Datainspektionen, som ska utöva tillsyn över Försvarsmaktens personuppgiftsbehandling inom Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst. Vid tillsyn har Datainspektionen rätt att få tillgång till de personuppgifter som behandlas, upplysningar om dokumentation av behandlingen av personuppgifter och säkerheten vid denna samt tillträde till sådana lokaler som har anknytning till behandlingen av personuppgifter (se närmare om detta i avsnitt 6.8.1).

Försvarsmakten hanterar årligen ärenden om begäran om information enligt FM-PuL[3], vilka sällan leder till annat än besked om att uppgifter som behandlas inom Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst omfattas av sekretess om det kan antas att det skadar Sveriges försvar eller på annat sätt vållar fara för rikets säkerhet om uppgifterna röjs. Även ett besked om att uppgifterna om en person *inte* förekommer i Försvarsmaktens försvarsunderrättelseverksamhet eller militära säkerhetstjänst kan vålla sådan skada. Därutöver lämnar Försvarsmakten generell information om i vilka ärendehanteringssystem och andra administrativa system som personuppgifter kan komma att behandlas enligt personuppgiftslagen.

Utredningen bedömer att rätten att begära information fortsatt är en viktig del i den enskildes rätt att i möjligaste mån informera sig om hur och i vilka sammanhang dennes personuppgifter behandlas. Även om det står klart att en begäran om sådan information, i vart fall inom Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst, sannolikt inte leder till annat än besked om att redan det förhållandet huruvida den enskildes personuppgifter förekommer i dessa verksamheter eller inte omfattas av sekretess, finns skäl att behålla denna begränsade möjlighet till insyn för den enskilde. Den föreslagna lagstiftningens utvidgade tillämpningsområde gör att denna möjlighet till insyn omfattar fler områden än tidigare.

[3] Att skilja från utlämningsärenden om allmänna handlingar. Försvarsmakten hanterade 43 ärenden om registerutdrag år 2015, 15 år 2016, 17 år 2017 och 8 till och med mars 2018.

6.7.3 Enskilds rätt till personrelaterad information hos Försvarets radioanstalt

Utredningens förslag: Försvarets radioanstalt är skyldig att till den som begär det utan onödigt dröjsmål en gång per kalenderår lämna skriftligt besked om personuppgifter som rör honom eller henne behandlas. Behandlas sådana uppgifter ska sökanden få del av dem och få följande skriftliga information.

1. Vilka personuppgifter om den sökande som behandlas.
2. Varifrån personuppgifterna kommer.
3. Den rättsliga grunden för behandlingen.
4. Ändamålen med behandlingen.
5. Mottagare eller kategorier av mottagare av personuppgifterna, även i annat land eller internationella organisationer.
6. Hur länge personuppgifterna får behandlas eller, om det inte är möjligt att ange, kriterierna för att fastställa det.
7. Rätten att begära rättelse, radering eller begränsning av behandlingen.

Sådant utlämnande behöver inte omfatta personuppgifter som sökanden har tagit del av, om inte han eller hon begär det. Det ska dock framgå av informationen att personuppgifterna i fråga behandlas.

Ansökan ska göras skriftligen hos Försvarets radioanstalt och vara undertecknad av den sökande själv. Information enligt första stycket ska 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.

Skäl för utredningens förslag: På samma sätt som Försvarsmakten är Försvarets radioanstalt enligt 2 kap. 1 § FRA-PuL skyldig att till var och en som ansöker om det en gång per kalenderår gratis lämna besked om huruvida personuppgifter som rör den sökande behandlas eller inte. En sökandes rätt enligt bestämmelsen att få reda på om personuppgifter som rör honom eller henne behandlas av Försvarets radioanstalt gäller inte i den utsträckning som sekretess hindrar att

uppgifterna lämnas ut till den registrerade, se vidare härom i avsnitt 6.7.4. Ovan angivna motivuttalanden om sekretess gäller även för Försvarets radioanstalts verksamhet och innebär på samma sätt som för Försvarsmakten att information sällan kommer lämnas ut, men att bestämmelser om information fyller en viktig funktion i de fall där sekretess inte gäller för uppgifterna.

Försvarets radioanstalt har hittills i samtliga ärenden om personrelaterad information som handlagts med stöd av FRA-PUL konstaterat att sekretess enligt 15 kap. 2 § offentlighets- och sekretesslagen (försvarssekretess) föreligger. Även uppgifter om att en person inte förekommer hos Försvarets radioanstalt har bedömts omfattas av nämnda sekretess. I samtliga dessa ärenden har sökanden således fått avslag på sin begäran, oavsett om det förekommer uppgifter om sökanden eller inte inom försvarsunderrättelse- och utvecklingsverksamheten. Enskilda har därmed inte kunnat kontrollera om eller i vilken omfattning det hos Försvarets radioanstalt behandlas personuppgifter om honom eller henne inom dessa verksamheter. Det kan mot denna bakgrund argumenteras för att bestämmelsen inte fyller den funktion som antagits under lagstiftningsprocessen vid införandet av FRA-PuL. I sammanhanget kan nämnas att Europadomstolen i ett avgörande den 19 juni 2018 om lagstiftningen om signalspaning i försvarsunderrättelseverksamhet i denna sak har funnit att ”the Court cannot find that it has practical importance”.

Av 5 kap. 1 § FRA-PuL och anslutande förordning framgår att Datainspektionen ska utöva tillsyn över Försvarets radioanstalts personuppgiftsbehandling inom försvarsunderrättelse- och utvecklingsverksamheten. Vid tillsyn har Datainspektionen på samma sätt som hos Försvarsmakten rätt att få tillgång till de personuppgifter som behandlas, upplysningar om dokumentation av behandlingen av personuppgifter och säkerheten vid denna samt tillträde till sådana lokaler som har anknytning till behandlingen av personuppgifter.

Mot bakgrund av den stränga sekretess som gäller för Försvarets radioanstalts verksamhet har det, utöver Datainspektionens tillsyn, införts särskild granskning till skydd för den personliga integriteten (prop. 2006/07:46 s. 101). Statens inspektion för försvarsunderrättelseverksamheten (Siun) har till uppgift att granska Försvarets radioanstalts personuppgiftsbehandling enligt FRA-PuL. Denna granskning inskränker inte Datainspektionens övergripande ansvar utan utgör en särskild granskning i syfte att kompensera för enskildas

begränsade möjlighet till insyn i personuppgiftsbehandlingen inom försvars- och utvecklingsverksamheten. Siun är även kontrollmyndighet enligt lagen om försvarsunderrättelseverksamhet och lagen om signalspaning i försvarsunderrättelseverksamhet.

Efter FRA-PuL:s tillkomst har det genom 10 a § lagen om signalspaning i försvarsunderrättelseverksamhet införts en möjlighet för enskilda att begära att Siun ska kontrollera om hans eller hennes meddelanden har inhämtats i samband med signalspaning och, om så är fallet, huruvida inhämtningen och behandlingen av inhämtade uppgifter har skett i enlighet med lag. Lagenligheten ska inte endast bedömas med utgångspunkt från lagen om signalspaning i försvarsunderrättelseverksamhet utan också från vad som är föreskrivet i fråga om behandling av personuppgifter (prop. 2008/09:201 s. 92). Kontrollen som Siun utför påminner om de sökningar som Försvarets radioanstalt utför efter ansökan enligt 2 kap. 1 § FRA-PuL. Siun ska underrätta den enskilde om att kontrollen har utförts.

Försvarets radioanstalt har mottagit få ansökningar om personalrelaterad information. Varje ansökan innebär emellertid en resurskrävande arbetsinsats vars resultat inte kommer att redovisas för den sökande med hänsyn till sekretess. Siuns kontroll enligt 10 a § lagen om signalspaning i försvarsunderrättelseverksamhet innebär också att Försvarets radioanstalts it-system söks igenom. Därutöver tillkommer att Försvarets radioanstalts personuppgiftsbehandling är föremål för tillsyn av Datainspektionen och särskild granskning av Siun. Detta talar för att behandlingen av personuppgifter inom Försvarets radioanstalt är föremål för en så omfattande och oberoende statlig kontroll att det kan ifrågasättas om möjligheten för enskilda att ansöka om personrelaterad information inom Försvarets radioanstalt försvarsunderrättelse- och utvecklingsverksamhet bör vara kvar. Att inte behålla möjligheten för enskilda att begära registerutdrag från Försvarets radioanstalt skulle dock innebära en inskränkning i, den i praktiken mycket begränsade, rätten att få del av information om myndighetens personuppgiftsbehandlingar. Att rätten sällan utnyttjas eller tillämpningen hittills inte har lett till något resultat för den enskilde bör inte föranleda att denna rättighet inskränks.

Eftersom tillämpningsområdet för den nya lagen föreslås utökas till att även avse informationssäkerhetsverksamheten, bör den föreslagna bestämmelsen även omfatta enskildas rätt till information som Försvarets radioanstalt behandlar inom denna verksamhetsgren.

6.7.4 Begränsning av rätten till information

Utredningens förslag: Informationsskyldigheten gäller inte i den utsträckning sekretess hindrar att uppgifterna lämnas ut. Om den förutsättningen är uppfylld är Försvarsmakten respektive Försvarets radioanstalt inte skyldig att lämna ut skälen för beslut om att inte lämna ut dessa uppgifter. Samma sak gäller beslut i fråga om rättelse, radering eller begränsning av behandlingen.

Informationsskyldigheten avseende information som ska lämnas om uppgifterna samlas in från personen själv samt information som ska lämnas efter begäran, gäller inte personuppgifter i löpande text som inte fått sin slutliga utformning när begäran gjordes eller som utgör minnesanteckning eller liknande. Informationsskyldigheten gäller dock om uppgifterna har lämnats ut till tredje part, behandlas enbart för vetenskapliga, statistiska eller historiska ändamål eller arkivändamål av allmänt intresse eller, när det gäller löpande text som inte fått sin slutliga utformning, om uppgifterna har behandlats längre än ett år.

Skäl för utredningens förslag: Enskildas rätt till information begränsas av bestämmelser om sekretess (2 kap. 4 § FM-PuL och 2 kap. 3 § FRA-PuL). Motiven finns i prop. 2006/07:46 s. 89. Liksom anfördes av regeringen i motiven till de nuvarande bestämmelserna om enskildas rätt till information, är många uppgifter som behandlas i Försvarsmaktens och Försvarets radioanstalts verksamheter till skydd för rikets säkerhet eller dess förhållande till andra stater eller mellanfolkliga organisationer (15 kap. 1 och 2 §§ offentlighets- och sekretesslagen). Den informationsskyldighet som föreslås i detta betänkande ska därför, på motsvarande sätt som enligt FM-PuL och FRA-PuL, inte gälla i den utsträckning sekretess hindrar att uppgifterna lämnas ut till den som uppgifterna rör. Eftersom skälen för beslut om sekretess kan ge ledning om uppgifternas innehåll, ska inte heller skälen för beslut om sekretess lämnas till den som gett in begäran. Redan uppgiften om huruvida en enskilds personuppgifter behandlas av Försvarsmakten eller Försvarets radioanstalt kan således omfattas av sekretess. Detsamma gäller frågor som rör rättelse, radering eller begränsning av behandling av personuppgifter i dessa sammanhang.

Av 2 kap. 3 § FM-PuL och 2 kap. 2 § FRA-PuL framgår att information som har begärts av en enskild inte behöver lämnas om

personuppgifter i löpande text som inte fått sin slutliga utformning när ansökan gjordes eller som utgör minnesanteckning eller liknande. 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. Motiven finns i prop. 2006/07:46 s. 87 f.

Motsvarande bestämmelser bör införas även i de nya lagarna.

6.7.5 Rätten till rättelse, radering och begränsning av behandlingen

Utredningens förslag: Försvarsmakten och Försvarets radioanstalt ska på begäran av den som personuppgiften rör snarast rätta, radera eller begränsa sådana personuppgifter som inte har behandlats i enlighet med de föreslagna lagarna eller föreskrifter som har meddelats med stöd av dessa lagar.

Försvarsmakten och Försvarets radioanstalt ska också underrätta tredje part till vilken uppgifterna har lämnats ut om åtgärden, om den som personuppgiften rör begär det eller om en mera betydande skada eller olägenhet för denne skulle kunna undvikas genom en underrättelse.

Någon underrättelse till tredje part behöver dock inte lämnas, om sekretess hindrar det eller detta är omöjligt eller skulle innebära en oproportionerligt stor arbetsinsats.

Skäl för utredningens förslag: Av 2 kap. 5 § FM-PuL och 2 kap. 4 § FRA-PuL framgår att Försvarsmakten respektive 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 meddelats med stöd av lagen. Myndigheterna ska 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 är omöjligt eller skulle innebära en oproportionerligt stor arbetsinsats. Motiven

finns i prop. 2006/07:46 s. 89 f. I det i avsnitt 6.7.3 beskrivna avgörandet av Europadomstolen har domstolen uttalat att ”that remedy must be deemed to be ineffective i practice”.

Vad som gäller enligt FM-PuL och FRA-PuL föreslås trots detta även gälla enligt de nya lagarna.

6.7.6 Avgifter samt beslut om avslag vid upprepad begäran

Utredningens förslag: Allmän information som Försvarsmakten och Försvarets radioanstalt ska göra tillgänglig samt information som Försvarsmakten ska lämna om uppgifterna samlas in från personen själv, ska lämnas av respektive myndighet utan avgift. Information som Försvarsmakten och Försvarets radioanstalt ska lämna efter begäran från den som uppgiften rör ska lämnas utan avgift en gång per kalenderår. Om någon begär sådan information om uppgifter oftare än en gång per kalenderår, får Försvarsmakten och Försvarets radioanstalt avslå begäran.

Skäl för utredningens förslag: Som angetts i avsnitt 6.7.2 och 6.7.3 är Försvarsmakten respektive Försvarets radioanstalt skyldig att till var och som ansöker om det, en gång per kalenderår gratis lämna besked om huruvida personuppgifter som rör den sökande behandlas eller inte (2 kap. 2 § FM-PuL och 2 kap. 1 § FRA-PuL). Hur en upprepad begäran inom samma kalenderår bör behandlas framgår emellertid inte av regeringens motiv till bestämmelserna. Utredningen anser att motsvarande bestämmelser ska införas även i de nya lagarna. De nya bestämmelserna bör dock göra det möjligt för Försvarsmakten respektive Försvarets radioanstalt att avslå upprepad begäran om registerutdrag, dvs. begäran som inkommer till myndigheterna oftare än en gång per kalenderår. En sådan begränsning inskränker inte rätten att begära ut allmänna handlingar. Ett beslut om avslag på grund av att begäran är upprepad bör inte kunna överklagas, se vidare avsnitt 6.9.2.

6.8 Tillsyn och kontroll

6.8.1 Tillsynsmyndighetens funktion, uppgifter och befogenheter

Utredningens förslag: Den myndighet som regeringen bestämmer ska utöva allmän tillsyn över Försvarsmaktens och Försvarets radioanstalts behandling av personuppgifter.

Tillsynsmyndigheten ska ge råd och stöd till Försvarsmakten och Försvarets radioanstalt om respektive myndighets skyldigheter enligt lag eller annan författning eller när det i övrigt är påkallat.

Tillsynsmyndigheten har rätt att av Försvarsmakten eller Försvarets radioanstalt eller ett personuppgiftsbiträde på begäran få

1. tillgång till personuppgifter som behandlas,
2. upplysningar om och dokumentation av behandlingen av personuppgifter och säkerhets- och skyddsåtgärder,
3. tillträde till sådana lokaler som har anknytning till behandling av personuppgifter och tillgång till utrustning och andra medel för behandling av personuppgifter, och
4. det biträde och annan information som behövs för tillsynen.

Om tillsynsmyndigheten bedömer att det finns risk för att personuppgifter kan komma att behandlas i strid med lag eller annan författning, ska myndigheten genom råd, rekommendationer eller påpekanden försöka förmå Försvarsmakten eller Försvarets radioanstalt eller personuppgiftsbiträdet att vidta åtgärder för att minska den risken.

Tillsynsmyndigheten får utfärda en skriftlig varning för att planerad behandling av personuppgifter riskerar att stå i strid med lag eller annan författning. Detsamma gäller om pågående behandling riskerar att stå i strid med lag eller annan författning.

Om tillsynsmyndigheten konstaterar att personuppgifter behandlas i strid med lag eller annan författning, eller att Försvarsmakten eller Försvarets radioanstalt eller ett personuppgiftsbiträde annars inte fullgör sina skyldigheter, får tillsynsmyndigheten

1. genom sådana åtgärder som anges i det föregående försöka förmå Försvarsmakten eller Försvarets radioanstalt eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsenlig eller att uppfylla andra skyldigheter,
2. förelägga Försvarsmakten eller Försvarets radioanstalt eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsenlig eller att fullgöra andra skyldigheter.

Om ett föreläggande utfärdas ska det av föreläggandet framgå när åtgärderna senast ska vara genomförda, och om det är lämpligt, vilka åtgärder som ska vidtas.

I förslaget till lag om behandling av personuppgifter vid Försvarets radioanstalt ska det tas in en bestämmelse som upplyser om att det i lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet finns särskilda bestämmelser om kontroll som rör Försvarets radioanstalts behandling av personuppgifter i försvarsunderrättelse- och utvecklingsverksamheten.

Skäl för utredningens förslag: Bestämmelser om tillsynsmyndighetens funktion, uppgifter och befogenheter finns i 5 kap. 1–4 §§ FM-PuL och FRA-PuL. Tillsynsmyndigheten har rätt att för sin tillsyn på begäran få,

1. tillgång till personuppgifter som behandlas,
2. upplysningar om och dokumentation av behandlingen av personuppgifter och säkerhets- och skyddsåtgärder,
3. tillträde till sådana lokaler som har anknytning till behandlingen av personuppgifter.
4. Om tillsynsmyndigheten konstaterar att personuppgifter behandlas eller kan komma att behandlas på ett olagligt sätt, ska myndigheten genom påpekanden eller liknande förfarande en försöka åstadkomma rättelse.

Tillsynsmyndigheten får hos förvaltningsrätten inom vars domkrets tillsynsmyndigheten är belägen ansöka om att sådana personuppgifter som har behandlats olagligt ska utplånas. Beslut om utplånande får inte meddelas om det är oskäligt.

Motiven finns i prop. 2006/07:46 s. 99 ff.

Utredningen anser att de bestämmelser som reglerar tillsyns- och kontrollmyndigheternas funktion, uppgifter och befogenheter enligt nuvarande lagstiftning bör föras in i de nya lagarna med undantag av möjligheten att hos förvaltningsrätten ansöka om utplåning av personuppgifter. Såvitt är känt för utredningen har något sådant inte förekommit eller varit aktuellt. I stället föreslår utredningen att om tillsynsmyndigheten i sin tillsyn uppmärksammar förhållanden som kan utgöra brott, ska myndigheten anmäla det till Åklagarmyndigheten. Bestämmelser om detta kan tas in i de förordningar som ska knyta an till lagarna.

Härutöver föreslår utredningen några tillägg i lagstiftningen.

Det bör uttryckligen framgå att tillsynsmyndigheten ska ge råd och stöd till Försvarsmakten och Försvarets radioanstalt om myndigheternas skyldigheter enligt lag eller annan författning eller när det i övrigt är påkallat. Det bör även framgå att tillsynsmyndigheten på begäran ska få upplysningar om och dokumentation av behandlingen av personuppgifter och säkerhets- och skyddsåtgärder vid behandlingen. Vidare bör tillsynsmyndigheten utöver rätten till tillträde till sådana lokaler som har anknytning till behandling av personuppgifter även få tillgång till utrustning och andra medel för behandling av personuppgifter. Slutligen bör tillsynsmyndigheten få det biträde och annan information som behövs för tillsynen.

Om tillsynsmyndigheten bedömer att det finns risk för att personuppgifter kan komma att behandlas i strid med lag eller annan författning, ska myndigheten genom råd, rekommendationer eller påpekanden försöka förmå den personuppgiftsansvarige att vidta åtgärder för att minska den risken.

Om en pågående eller planerad behandling av personuppgifter riskerar att stå i strid med lag eller annan författning får tillsynsmyndigheten utfärda en skriftlig varning.

Om tillsynsmyndigheten konstaterar att personuppgifter behandlas i strid med lag eller annan författning, eller att den personuppgiftsansvarige annars inte fullgör sina skyldigheter, får tillsynsmyndigheten försöka förmå eller förelägga den personuppgiftsansvarige att vidta åtgärder för att behandlingen ska bli författningsenlig eller att uppfylla eller fullgöra andra skyldigheter.

6.8.2 Rapporteringsskyldighet för personuppgiftsincidenter bör inte införas i de nya lagarna

Utredningens bedömning: Bestämmelser om särskild rapporteringsskyldighet av personuppgiftsincidenter till tillsynsmyndigheten och den som personuppgifterna rör, bör inte införas i de nya lagarna.

Skäl för utredningens bedömning: Personuppgiftsincident är ett nytt begrepp som varken har funnits i tidigare personuppgiftslagar eller FM-PuL respektive FRA-PuL. Bestämmelser om rapporteringsskyldighet och hantering av personuppgiftsincidenter finns därför inte.

En personuppgiftsincident är enligt artikel 3.11 i 2016 års dataskyddsdirektiv en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats. Begreppet definieras följaktligen på samma sätt i de lagar som föreslagits med anledning av direktivet; bl.a. brottsdatalagen.

I brottsdatalagen regleras den personuppgiftsansvariges skyldigheter vid en personuppgiftsincident. Där föreskrivs bl.a. att sådana incidenter ska anmälas till tillsynsmyndigheten inom viss tid och att den registrerade i vissa fall ska underrättas om incidenten. Enligt de föreslagna bestämmelserna ska anmälningsskyldigheten inte gälla om personuppgiftsincidenten rör nationell säkerhet (3 kap. 9–11 §§). Enligt förslaget till Säkerhetspolisens datalag ska sådan rapporteringsskyldighet inte heller gälla för Säkerhetspolisen (SOU 2017:74 s. 684). I 1 kap. 4 § dataskyddslagen har regleringen rörande rapportering av dataskyddsincidenter i dataskyddsförordningen (art. 33 och 34) undantagits ifråga om personuppgiftsincidenter som rapporteras enligt säkerhetsskyddslagen eller föreskrifter som meddelats i anslutning till den lagen. Detta innebär att sådana incidenter som ska rapporteras enligt 10 a § första stycket säkerhetsskyddsförordningen ska anmälas till den myndighet som utövar tillsyn över säkerhetsskyddet, dvs. Försvarsmakten eller Säkerhetspolisen, inte också ska rapporteras till tillsynsmyndigheten enligt dataskyddsförordningen.

Personuppgiftsincidenter som inträffar i Försvarsmaktens och Försvarets radioanstalts informationssystem och som drabbar personuppgifter som behandlas med stöd av de föreslagna lagarna kommer att röra nationell säkerhet. Sådana personuppgiftsincidenter hos Försvarsmakten och Försvarets radioanstalt kommer således att rapporteras i enlighet med vad som framgår av säkerhetsskyddsförordningen. Något behov av att införa särskilda bestämmelser om rapportering av personuppgiftsincidenter i de nya lagarna finns därmed inte.

6.8.3 Sanktionsavgift bör inte få tas ut

Utredningens bedömning: Det bör inte tas in bestämmelser om sanktionsavgift i de nya lagarna om personuppgiftshantering hos Försvarsmakten och Försvarets radioanstalt.

Skäl för utredningens bedömning: Av 2016 års dataskyddsdirektiv följer att medlemsstaterna ska föreskriva sanktioner för överträdelser av de bestämmelser som genomför direktivet och att sanktionerna ska vara effektiva, proportionerliga och avskräckande. I brottsdatalagen införs ett nytt system med administrativa sanktionsavgifter där tillsynsmyndigheten ska fatta beslut om sanktionsavgift.

Även EU:s dataskyddsförordning föreskriver att administrativa sanktionsavgifter ska kunna tas ut vid överträdelse av bestämmelser om personuppgiftsbehandling som sker inom ramen för verksamhet som regleras av denna förordning. Enligt 6 kap. 2 § dataskyddslagen kan tillsynsmyndigheten även ta ut en sanktionsavgift av en myndighet vid överträdelse av dataskyddsförordningen.

Huvudskälet till att Utredningen om 2016 års dataskyddsdirektiv föreslog att sanktionsavgift ska kunna tas ut av bl.a. Polismyndigheten, Skatteverket, Tullverket och domstolarna, är att motsvarande sanktionssystem gäller enligt dataskyddsförordningen och att för flera av myndigheterna kommer sannolikt en större del av personuppgiftsbehandlingen att regleras av dataskyddsförordningen. Utredningen ansåg att det var svårt att motivera att helt olika sanktionssystem ska gälla beroende på om brottsdatalagen eller förordningen var tillämplig vid överträdelser som är likartade och som därför kan antas motivera samma sanktion (SOU 2017:29 s. 492). Utredningen

föreslog dock inte att sanktionsavgifter skulle kunna tas ut av Säkerhetspolisen. Som skäl anfördes att Säkerhetspolisens verksamhet rör nationell säkerhet och därmed inte omfattas av vare sig dataskyddsdirektivets eller dataskyddsförordningens tillämpningsområde

Till en början kan konstateras att de krav på sanktionsavgifter som unionsrätten ställer inte gäller för de behandlingar av personuppgifter som regleras i den lagstiftning som utredningen lägger fram i detta betänkande.

Dataskyddskonventionen (se avsnitt 4.2.1) som även omfattar personuppgiftsbehandling som rör nationell säkerhet, ställer krav på att det ska finnas lämpliga sanktioner och rättsmedel för överträdelser av bestämmelser om dataskydd, men anger inte närmare vilka krav som ställs på sådana sanktioner.

Den nuvarande regleringen ger möjlighet till skadestånd. Utredningen föreslår ingen ändring i detta avseende. Vidare kan straffrättsligt ansvar utkrävas enligt brottsbalken. Utöver Datainspektionens tillsynsverksamhet kontrollerar Statens inspektion för försvarsunderrättelseverksamheten (Siun) försvarsunderrättelseverksamheten och granskar behandlingen av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst samt Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet När det gäller signalspaningen finns bestämmelser som är av intresse i detta sammanhang i lagen om signalspaning i försvarsunderrättelseverksamheten. Signalspaningsmyndigheten (Försvarets radioanstalt) ska ansöka om tillstånd hos Försvarsunderrättelsedomstolen för signalspaning (4 a §). Kontrollmyndigheten (Siun) får besluta att viss inhämtning ska upphöra eller att upptagning eller uppteckning av inhämtade uppgifter ska förstöras, om det vid kontroll framkommer att inhämtningen inte är förenlig med tillstånd som har meddelats enligt lagen (10 §). Vidare är kontrollmyndigheten skyldig att på begäran av en enskild kontrollera om hans eller hennes meddelanden har inhämtats i samband med signalspaning och, om så är fallet, huruvida inhämtningen och behandlingen har skett i enlighet med lag (10 a §). Mot bakgrund av den tillsyn, kontroll och granskning som gäller för de verksamheter som de föreslagna lagarna omfattar anser utredningen att konventionens krav på lämpliga sanktioner och rättsmedel är uppfyllda.

Enligt utredningens mening är de sanktionsmöjligheter som föreslås gälla i fortsättningen tillräckliga. Utredningen anser därför att

det inte bör införas någon möjlighet att ta ut sanktionsavgift vid överträdelse av bestämmelser i de nya lagarna.

6.9 Skadestånd och överklagande

6.9.1 Skadestånd

Utredningens förslag: Den personuppgiftsansvarige ska ersätta den som en personuppgift rör för den skada och kränkning av den personliga integriteten som orsakats av behandling av personuppgiften i strid med de föreslagna lagarna, eller föreskrifter som har meddelats i anslutning till dem.

Ersättningsskyldigheten kan jämkas i den utsträckning det är skäligt, om den personuppgiftsansvarige visar att felet inte berodde på denne.

Skäl för utredningens förslag: Enligt 2 kap. 6 § FM-PuL och 2 kap. 5 § FRA-PuL ska staten ersätta den registrerade för skada och kränkning av den personliga integriteten som en behandling av personuppgifter i strid med dessa lagar eller föreskrifter som har meddelats med stöd av lagarna har orsakat. Enligt bestämmelsens andra stycke kan ersättningsskyldigheten i den utsträckning det är skäligt jämkas, om Försvarsmakten respektive Försvarets radioanstalt visar att felet inte berodde på myndigheten.

Motiven finns i prop. 2006/07:46 s. 90 ff.

Utredningen anser att motsvarande bestämmelser bör införas i de nya lagarna.

Av bestämmelserna i FM-PuL och FRA-PuL framgår att det är staten som ska ersätta den drabbade vid felaktig behandling av personuppgifter.

Enligt 3 § förordningen (1995:1301) om handläggning av skadeståndsanspråk mot staten handlägger Justitiekanslern anspråk på ersättning enligt 2 kap. 6 § FM-PuL och 2 kap. 5 § FRA-PuL. Detta innebär att Försvarsmakten och Försvarets radioanstalt ska överlämna ersättningsanspråk med anledning av personuppgiftshantering enligt FM-PuL och FRA-PuL till Justitiekanslern för vidare hantering och beslut. För det fall den som personuppgifterna rör vänder sig till domstol för Justitiekanslern statens talan i saken.

Oavsett om Justitiekanslern eller domstolen fattar beslut om ersättning överlämnar Justitiekanslern med stöd i 2 a § förordningen (1975:1345) med instruktion för Justitiekanslern, till den myndighet som är berörd i skaderegleringsärendet att ansvara för att ersättningsbelopp betalas ut till motparten.

6.9.2 Överklagande av en myndighets beslut i egenskap av personuppgiftsansvarig

Utredningens förslag: Försvarsmaktens och Försvarets radioanstalts beslut om information som ska lämnas efter begäran av en enskild och om rättelse och underrättelse till tredje part samt Försvarsmaktens beslut om information som ska lämnas om uppgifter samlas in från personen själv, får överklagas hos allmän förvaltningsdomstol. Andra beslut enligt lagen får inte överklagas. Prövningstillstånd krävs vid överklagande till kammarrätten.

Beslut i frågor om sekretess överklagas till kammarrätt.

Skäl för utredningens förslag: Försvarsmaktens respektive Försvarets radioanstalts beslut beträffande information som ska lämnas om uppgifterna samlas in från personen själv (endast Försvarsmakten) samt efter begäran (Försvarsmakten och Försvarets radioanstalt) och om rättelse och underrättelse till tredje man får enligt 6 kap. 3 § FM-PuL och FRA-PuL överklagas hos allmän förvaltningsdomstol. Andra beslut som har meddelats med stöd av respektive lag får inte överklagas.

Som tidigare har anförts bör fysiska personer av integritetsskyddsskäl ha vissa grundläggande rättigheter som rör behandlingen av uppgifter om dem. Förutom rätt till information, rättelse och skadestånd, bör också vissa beslut av Försvarsmaktens och Försvarets radioanstalts beslut kunna överklagas.

Som framgått i tidigare avsnitt föreslås att de bestämmelser i FM-PuL och FRA-PuL som ger enskilda rätt till information efter ansökan samt rättelse och underrättelse till tredje part, med vissa justeringar och tillägg, ska införas även i de nya lagarna. Därför bör enligt utredningen Försvarsmaktens och Försvarets radioanstalts beslut i dessa frågor kunna överklagas till allmän förvaltningsdomstol på samma sätt som enligt FM-PuL och FRA-PuL. Den begränsning

som föreslås, om att Försvarsmakten och Försvarets radioanstalt får avslå sådan begäran om registerutdrag som enskild lämnar vid fler än ett tillfälle per kalenderår, begränsar endast enskilds rätt att ta del av information. Försvarsmaktens och Försvarets radioanstalts initiala prövning i dessa frågor blir huruvida en sådan begäran inkommit vid tidigare tillfälle innevarande kalenderår. Om så är fallet kommer en sådan begäran leda till ett omedelbart beslut om avslag. En sådan prövning är närmast att betrakta som av processuell karaktär och någon rätt till särskild överprövning av sådana beslut föreslås därför inte.

I klargörande syfte föreslås även att det upplyses om att beslut om sekretess överklagas till kammarrätt (se Högsta förvaltningsdomstolens avgörande i HFD 2014 ref 55).

6.10 Övriga bestämmelser

6.10.1 Straff

Utredningens bedömning: Överträdelser av bestämmelserna om personuppgiftsbehandling bör inte vara straffsanktionerade utöver vad som gäller enligt brottsbalken.

Skäl för utredningens bedömning: Bestämmelser om straff för vissa gärningar i samband med personuppgiftshantering regleras särskilt i 6 kap. 2 § FM-PuL och FRA-PuL. Den som uppsåtligen eller av grov oaktsamhet lämnar osann uppgift i information till den som personuppgiften rör, till tillsynsmyndigheten eller behandlar känsliga uppgifter i strid med vad som gäller enligt de särskilda bestämmelserna för den behandlingen. Straffet kan vara böter eller fängelse i högst sex månader, eller om brottet är grovt, till fängelse i högst två år. I ringa fall döms inte till ansvar.

Av skälen till regeringens förslag om införande av straffbestämmelser framgår att bestämmelserna om straff vid visst förfarande med personuppgifter har sitt ursprung i motsvarande bestämmelser i personuppgiftslagen. Enligt regeringens uttalanden fyller införande av straffbestämmelser en viktig funktion för att markera allvaret i överträdelser av regler till skydd för enskildas integritet. Regeringen ansåg därför att straffbestämmelser motsvarande delar av 49 § personuppgiftslagen även skulle intas i FM-PuL och FRA-PuL (prop. 2006/07:46 s. 107).

Behandling av personuppgifter i strid med lag kan föra med sig skyldighet för staten att betala skadestånd till de drabbade. Presumtionen för att skadestånd ska utgå liksom tillsynen och kontrollen bör enligt utredningen utgöra tillräckligt skydd för enskildas integritet. Utredningen anser att straffbestämmelserna i den del som avser utlämning av personuppgifter till tillsyns- och kontrollmyndigheterna inte bör föras över till de nya lagarna eftersom de skärpta formuleringarna om insyn och biträde för tillsynsmyndigheterna gör att utrymmet att lämna osanna uppgifter till tillsynsmyndigheten får betraktas som litet. Härtill bör beaktas att de nuvarande reglerna inte riktas mot vare sig den personuppgiftsansvarige eller personuppgiftsbiträden, utan mot den enskilde befattningshavaren, vars gärningar dessutom redan omfattas av reglerna om tjänstefel i 20 kap. 1 § brottsbalken. Överträdelser kan dessutom vara resultatet av flera personers agerande och underlåtenhet. Det blir då svårt att visa var skulden ligger och vad som lett till överträdelsen.

Utredningen anser mot bakgrund av det anförda att straffbestämmelserna i FM-PuL och FRA-PuL inte bör tas in i de nya lagarna.

6.11 Övergångsbestämmelser

Utredningens förslag: De föreslagna lagarna och de till dem knutna förordningarna ska träda i kraft den 1 oktober 2019.

Bestämmelserna om loggning behöver inte tillämpas på uppgiftssamlingar som inrättats före ikraftträdandet förrän den 1 maj 2024.

Ärenden om tillsyn eller granskning som inte har avgjorts före ikraftträdandet handläggs enligt äldre föreskrifter.

Skäl för utredningens förslag: Med hänsyn till den tid som krävs för remissbehandling, beredning inom Regeringskansliet samt riksdagsbehandling, bör de nya lagarna och förordningarna träda i kraft den 1 oktober 2019.

Det kommer att ta tid att anpassa de uppgiftssamlingar som har inrättats före den 1 oktober 2019 till bestämmelserna om loggning. Av den anledningen bör bestämmelserna inte tillämpas på sådana uppgiftssamlingar förrän den 1 maj 2024.

Ärenden om tillsyn eller granskning av Försvarsmaktens eller Försvarets radioanstalts personuppgiftsbehandling som Datainspektionen eller Statens inspektion för försvarsunderrättelseverksamheten inte har avgjort före ikraftträdandet bör handläggas enligt äldre föreskrifter.

6.12 Ändringar i andra författningar till följd av utredningens förslag

6.12.1 Ändring i lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning

Utredningens förslag: Undantaget i dataskyddslagen från bestämmelsen i den lagen som utsträcker dataskyddsförordningens tillämpningsområde ändras till att gälla lagarna om behandling av personuppgifter vid Försvarsmakten och Försvarets radioanstalt.

Skäl för utredningens förslag: I avsnitt 6.1.1 föreslår utredningen att FM-PuL och FRA-PuL ersätts med två nya lagar. Den bestämmelse om undantag från dataskyddsförordningen som finns i 1 kap. 3 § dataskyddslagen bör därför ändras och utformas i enlighet med detta, dvs. att undantaget gäller de nya lagarna.

6.12.2 Ändring i brottsdatalagen (2018:1177)

Utredningens förslag: Undantaget i brottsdatalagen från sådan verksamhet som omfattas av lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelse-verksamhet och militära säkerhetstjänst ändras till att gälla lagen om behandling av personuppgifter vid Försvarsmakten.

Skäl för utredningens förslag: I avsnitt 6.1.1 föreslår utredningen bl.a. att FM-PuL ersätts med en ny lag. Den bestämmelse om undantag från brottsdatalagen i 1 kap. 4 § andra stycket brottsdatalagen bör därför ändras och utformas i enlighet med detta, dvs. att undantaget gäller den nya lagen.

6.12.3 Ändring i lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet

Utredningens förslag: I bestämmelsen i 2 a § lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet om att inhämtning inte får avse signaler mellan en avsändare och mottagare som båda befinner sig i Sverige införs i bestämmelsens andra stycke ett undantag i fråga om signaler som utväxlas autonomt mellan tekniska system i sådana fall där signalerna inte innehåller personuppgifter.

Hänvisningen i 12 a § samma lag till lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet ändras till att avse lagen om behandling av personuppgifter vid Försvarets radioanstalt.

Skäl för utredningens förslag: Utredningen har uppmärksammats på en lagbestämmelse som avser att främja integritetsskyddsintresset har fått en räckvidd som inverkar menligt på för försvaret viktiga verksamheter och där några sådana intressen av tekniska skäl inte kan förekomma.

Bestämmelsen i fråga är 2 a § lagen om signalspaning i försvarsunderrättelseverksamhet. Enligt den får inhämtning inte avse signaler mellan en avsändare och mottagare som båda befinner sig i Sverige. Om sådana signaler inte kan avskiljas redan vid inhämtningen, ska upptagningen eller uppteckningen förstöras så snart det står klart att sådana signaler har inhämtats. I paragrafens andra stycke undantas från denna bestämmelse signaler mellan sändare och mottagare på utländska statsfartyg, luftfartyg och militära fordon.

Föreskrifterna i 2 a § gäller såväl kommunikationsspaning (mänsklig kommunikation) som teknisk signalspaning.

Den tekniska signalspaningen riktar in sig på egenskaper hos tekniska signaler, dvs. sådana signaler som inte bär mänsklig kommunikation. Denna signalspaning syftar till att beskriva signalers olika tekniska parametrar, exempelvis pulsfrekvens och amplitud.

Radarsignaler är exempel på tekniska signaler som utväxlas autonomt i och mellan tekniska system och där det inte finns några inslag av mänsklig kommunikation eller information och där det därför inte kan uppkomma frågor om personlig integritet.

Radar är utrustning som skickar ut elektromagnetiska pulser och som tar emot reflektionen av de utskickade signalerna. Radar används främst för att mäta avstånd och riktning till objekt i omgivningen. Mätningen görs oftast genom att en puls skickas ut. Pulsen studsar sedan mot något och fångas därefter in av radarn. Sändare och mottagare finns alltså i samma tekniska utrustning. Genom att mäta tiden det tar för pulsen att komma tillbaka samt övervaka i vilken riktning pulsen skickas ut kan man avgöra avståndet och riktningen till objektet. En radarsignal innehåller endast tekniska parametrar, t.ex. frekvens, och alltså, som nyss nämnts, inte information med mänsklig kommunikation.

Försvarets radioanstalt inhämtar och analyserar radarsignaler inom ramen för den tekniska signalspaningen i syfte att identifiera dem och associera dem till det objekt (plattform eller farkost) de härrör från.

Inhämtningen av radarsignaler är av betydelse för uppbyggnaden och vidmakthållandet av det s.k. signalreferensbiblioteket som Försvarets radioanstalt enligt 3 c § förordningen med instruktion för Försvarets radioanstalt har till uppgift att vidmakthålla och utveckla för Försvarsmaktens behov. Användningen av detta har stor betydelse för Försvarsmaktens möjligheter att identifiera farkoster och vapenbärare av olika slag och för bedömningar om vilket hot dessa i varje givet ögonblick kan utgöra för Försvarsmaktens plattformar och personal. För detta syfte är det nödvändigt att biblioteket innehåller uppgifter om såväl utländska som inhemska signaler, civila som militära. Som anförs i förarbetena till 2 a § kan inhämtning av den här typen av signaler från Försvarsmaktens utrustningar och plattformar ske med samtycke från Försvarsmakten, även när de befinner sig i Sverige (prop. 2008/09:201). När det gäller signaler mellan sändare och mottagare på utländska statsfartyg, luftfartyg och militära fordon som befinner sig i Sverige är inhämtning likaledes möjlig enligt undantagsregeln i andra stycket.

I andra fall är det enligt bestämmelsen i 2 a § otydligt huruvida det är möjligt att mäta signaler som emanerar från svenskt territorium. Vad gäller radarsignaler kan man hävda att eftersom samma radarsignal utgår och återkommer till samma radarutrustning så är det inte fråga om signaler mellan avsändare och mottagare av det slag som avses med 2 a §, och därmed inte heller signaler mellan en avsändare och mottagare som befinner sig i Sverige. Ett annat synsätt

är att det objekt som radarsignalen studsar mot är att betrakta som sändare. Det är dock den som sänder ut radarsignalen, inte Försvarets radioanstalt, som kan registrera på vilket objekt som signalen studsar.

Även i andra sammanhang än vid teknisk signalspaning till stöd för produktion av signalreferensbibliotek förekommer signaler som utväxlas autonomt i och mellan tekniska system där ingen mänsklig information förekommer och där inga integritetsaspekter gör sig gällande. Inte heller i dessa sammanhang gör sig de integritetshänsyn som avsändare-mottagare-begreppet adresserar gällande.

Som framgår ovan innehåller de beskrivna signalerna inte uppgifter om mänsklig kommunikation och inhämtningen har därmed ingen betydelse för personrelaterad integritet. Utredningen föreslår därför att undantagsregeln i andra stycket kompletteras med ett undantag som innebär att huvudregeln i första stycket inte tillämpas i fråga om signaler som utväxlas autonomt mellan tekniska system och inte innehåller personuppgifter.

Bestämmelsen i 12 a § lagen om signalspaning i försvarsunderrättelsetjänst hänvisar till lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet för ytterligare bestämmelser om behandlingen av inhämtade personuppgifter. Denna hänvisning bör ändras så att den avser lagen om personuppgiftsbehandling vid Försvarets radioanstalt.

6.12.4 Ändring i förordningen (2009:969) med instruktion för Statens inspektion för försvarsunderrättelseverksamheten

Utredningens förslag: Bestämmelserna i instruktionen för Statens inspektion för försvarsunderrättelseverksamheten om att inspektionen ska granska behandlingen av personuppgifter som sker med stöd av FM-PuL och FRA-PuL utformas så att de direkt tar sikte på den behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst som sker med stöd av lagen (2019:000) om behandling av personuppgifter vid Försvarsmakten och den behandling av personuppgifter i

Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet som sker med stöd av lagen (2019:000) om behandling av personuppgifter vid Försvarets radioanstalt.

Inspektionen ska utöver uppgiften att utöva kontroll och granskning även ha till uppgift att lämna myndigheterna råd och stöd beträffande myndigheternas skyldigheter i den verksamhet som inspektionen har till uppgift att kontrollera och granska.

Skäl för utredningens förslag: Statens inspektion för försvarsunderrättelseverksamheten (Siun) har enligt 1 § förordningen med instruktion för Statens inspektion för försvarsunderrättelseverksamheten till uppgift att kontrollera försvarsunderrättelseverksamheten hos de myndigheter som enligt förordningen (2000:131) om försvarsunderrättelseverksamhet bedriver sådan verksamhet. Siun ska kontrollera att dessa myndigheter i den försvarsunderrättelseverksamhet som utförs, efterlever lagar och förordningar samt i övrigt fullgör sina skyldigheter.

Siun ska vidare enligt 3 § instruktionen granska behandlingen av uppgifter enligt FM-PuL och FRA-PuL.

Med hänsyn till de föreslagna lagarnas vidgade tillämpningsområden bör hänvisningarna i dem om behandling av personuppgifter utformas så att de direkt tar sikte på försvarsunderrättelseverksamheten och den militära säkerhetstjänsten vid Försvarsmakten och försvarsunderrättelse- och utvecklingsverksamheten vid Försvarets radioanstalt.

Siuns tillsyns- och granskningsuppdrag avser rättslig granskning i efterhand. Det innebär att planerade åtgärder hos myndigheterna inte kan bli föremål för granskning och att Siuns verksamhet inte kan uppfattas som ett godkännande av framtida åtgärder. Det bör dock finnas ett utrymme för överväganden som kan komma att påverka den framtida personuppgiftsbehandlingen. Enligt utredningens mening skulle det vara värdefullt för myndigheterna att, med den begränsning som nyss berörts, kunna få råd och stöd beträffande deras skyldigheter i de verksamheter som Siun har till uppgift att granska. Förslaget överensstämmer med det som lämnas när det gäller tillsynsmyndigheten i avsnitt 6.8.1.

6.12.5 Ändring i förordningen (1995:1301) om handläggning av skadeståndsanspråk mot staten

Utredningens förslag: Föreskrifterna i 3 § förordningen (1995:1301) om handläggning av skadeståndsanspråk mot staten att Justitiekanslern handlägger anspråk på ersättning med stöd av 2 kap. 6 § FM-PuL och 2 kap. 5 § FRA-PuL ändras till att avse anspråk på ersättning med stöd av 7 kap. 1 § i lagen om behandling av personuppgifter vid Försvarsmakten och 7 kap. 1 § lagen om behandling av personuppgifter vid Försvarets radioanstalt.

Skäl för utredningens förslag: I 3 § förordningen om handläggning av ersättningsanspråk mot staten anges att Justitiekanslern handlägger anspråk på ersättning bl.a. med stöd av 2 kap. 6 § FM-PuL och 2 kap. 5 § FRA-PuL. Bestämmelsen bör ändras så att den avser motsvarande föreskrifter i de nya lagarna.

7 Konsekvenser

7.1 Inledning

I kommittéförordningen (1998:1474) finns bestämmelser om konsekvensbeskrivningar.

Av 14 § framgår att om förslagen i ett betänkande påverkar kostnaderna eller intäkterna för staten, kommuner, landsting, företag eller andra enskilda, ska en beräkning av dessa konsekvenser redovisas i betänkandet. Om förslagen innebär samhällsekonomiska konsekvenser i övrigt, ska dessa redovisas. När det gäller kostnadsökningar och intäktsminskningar för staten, kommuner eller landsting, ska kommittén föreslå en finansiering.

Av 15 § framgår att om förslagen i ett betänkande har betydelse för den kommunala självstyrelsen, för brottsligheten och det brottsförebyggande arbetet, för sysselsättning och offentlig service i olika delar av landet, för små företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt i förhållande till större företags, för jämställdheten mellan kvinnor och män eller för möjligheterna att nå de integrationspolitiska målen, ska konsekvenserna i det avseendet anges i betänkandet.

Om ett betänkande innehåller förslag till nya eller ändrade regler, ska förslagens kostnadsmässiga och andra konsekvenser anges i betänkandet. Konsekvenserna ska anges på ett sätt som motsvarar de krav på innehållet i konsekvensutredningar som finns i 6 och 7 §§ förordningen (2007:1244) om konsekvensutredning vid regelgivning (15 a §).

Enligt utredningens direktiv ska utredaren bedöma de ekonomiska konsekvenserna av förslagen för det allmänna och för enskilda. Om förslagen kan förväntas leda till kostnadsökningar för det allmänna ska utredaren föreslå hur de ska finansieras. Utredaren ska

också redovisa förslagens konsekvenser för den personliga integriteten och för eventuella verksamhetsmässiga konsekvenser.

7.2 Konsekvenser av förslagen

7.2.1 Två nya lagar men inga nya uppgifter

Utredningens bedömning: De föreslagna lagarna innebär inga nya uppgifter för Försvarsmakten eller Försvarets radioanstalt. De kommer att leda till ökad tydlighet och förbättrad effektivitet.

Skäl för bedömningen: De föreslagna lagarna innebär inga nya uppgifter för Försvarsmakten eller Försvarets radioanstalt. De ansluter till stora delar vad som gäller i dag genom FM-PuL och FRA-Pul samt PuL. I vissa delar medför förslagen förtydliganden och förbättringar när det gäller behandlingen av personuppgifter i försvarsunderrättelseverksamheten. Ökade möjligheter för direktåtkomst för Försvarsmakten, Försvarets radioanstalt och Säkerhetspolisen i försvarsunderrättelseverksamheten bör öka myndigheternas effektivitet på det området. För Försvarsmaktens del innebär ökade möjligheter till annat elektroniskt informationsutbyte förbättringar för verksamheten. Regleringen för vilka andra ändamål än huvudändamålen som behandling av personuppgifter får ske i Förvarets radioanstalts verksamheter innebär förtydliganden som är av godo såväl för myndigheten som för tillsynen och kontrollen.

7.3 Ekonomiska konsekvenser

Utredningens bedömning: De föreslagna lagarna innebär inga ökade kostnader för Försvarsmakten, Försvarets radioanstalt eller de myndigheter som utövar tillsyn och kontroll eller i övrigt för det allmänna. De har ingen ekonomisk betydelse för enskilda.

Skäl för bedömningen: De föreslagna lagarna medför inga nya uppgifter för Försvarsmakten och Försvarets radioanstalt. De nya reglerna kan medföra ett visst behov av utbildning av myndigheternas personal utöver den utbildningsverksamhet som myndigheterna

redan nu bedriver. De kostnader som detta kan medföra bör kunna rymmas inom myndigheternas befintliga ekonomiska ramar. Som nämnts i avsnitt 7.2.1 kan de föreslagna lagarna medföra förbättringar av myndigheternas effektivitet.

Några ekonomiska konsekvenser i övrigt för det allmänna uppkommer inte. Inte heller medför förslagen ekonomiska konsekvenser för enskilda.

7.3.1 Konsekvenser för den personliga integriteten

Utredningens bedömning: Sammantaget innebär förslagen att skyddet för den personliga integriteten kommer att vara på samma nivå som för närvarande. I viss mån kan intrånget i personlig integritet öka genom de ökade möjligheterna till direktåtkomst som motiveras av starka försvars- och säkerhetsintressen.

Skäl för bedömningen: När det gäller Försvarsmakten innebär en samlad reglering en förenkling för myndigheten och därmed i förlängningen en förstärkning av integritetsskyddet vid myndighetens behandling av personuppgifter.

Regleringen för vilka andra ändamål än huvudändamålen som behandling av personuppgifter får ske i Förvarets radioanstalts verksamheter är även till fördel från integritetskyddssynpunkt.

De effektiviseringar som föreslås för försvarsunderrättelseverksamheten och den militära säkerhetstjänsten, främst när det gäller möjligheter till direktåtkomst, kan innebära ett visst ytterligare intrång i den personliga integriteten. Samtidigt måste man beakta den säkerhetspolitiska utvecklingen på senare tid och de hot som riktas och som kan komma att riktas mot vårt land och de människor som finns här. Integritetsintrånget måste därför ställas mot de starka försvars- och säkerhetsintressen som här gör sig gällande och som motiverar behovet av en effektiv verksamhet på de områden som de föreslagna lagarna omfattar.

Att dataskyddsförordningens och dataskyddslagens bestämmelser om tillsynsmyndighetens befogenhet att förbjuda behandling inte ska gälla kan uppfattas som negativt för skyddet av enskildas personliga integritet. Detsamma gäller att personuppgiftsincidenter

inte ska rapporteras till tillsynsmyndigheten och att sanktionsavgifter inte ska få tas ut. Med hänsyn till den betydelse myndigheternas verksamhet har för Sveriges försvar och säkerhet är det olämpligt med föreskrifter om förbud mot behandling, rapportering av personuppgiftsincidenter och sanktionsavgifter. När det gäller frågan om rapportering av personuppgiftsincidenter bör erinras om den skyldighet att rapportera it-incidenter enligt 10 a § säkerhetskyddsförordningen som ska gälla i stället. I avsnitt 6.8.1–6.8.3 redovisar utredningen de bestämmelser om tillstånd, kontroll, granskning och tillsyn som gäller och ska gälla för den behandling av personuppgifter som den föreslagna lagstiftningen omfattar. Enligt utredningens mening får dessa bestämmelser anses tillgodose intresset av integritetsskydd.

7.3.2 Konsekvenser i övrigt

Utredningens bedömning: Förslagen förväntas inte få några andra konsekvenser.

Skäl för bedömningen: Förslagen får inte några samhällsekonomiska konsekvenser eller några konsekvenser för den kommunala självstyrelsen. Förslagen får inte heller några konsekvenser för jämställdheten eller andra sådana konsekvenser som avses i 14, 15 och 15 a §§ kommittéförordningen.

8 Författningskommentar

8.1 Förslaget till lag om behandling av personuppgifter vid Försvarsmakten

1 kap. Allmänna bestämmelser

Syftet med lagen

1 §

Syftet med denna lag är att säkerställa att Försvarsmakten kan behandla personuppgifter på ett ändamålsenligt sätt och att skydda fysiska personers grundläggande fri- och rättigheter i samband med sådan behandling.

Paragrafen, som behandlas i avsnitt 6.2.1, anger syftet med lagen. Syftet är att säkerställa att Försvarsmakten kan behandla personuppgifter på ett ändamålsenligt sätt och att skydda fysiska personers grundläggande fri- och rättigheter i samband med sådan behandling. Av paragrafen framgår att lagen gäller fysiska personer och inte juridiska personer.

Lagens tillämpningsområde

2 §

Denna lag gäller vid Försvarsmaktens behandling av personuppgifter som rör Sveriges försvar och säkerhet.

Paragrafen reglerar, tillsammans med 3 §, lagens tillämpningsområde. Den behandlas i avsnitt 6.2.2.

I paragrafen anges att lagen gäller vid Försvarsmaktens behandling av personuppgifter som rör Sveriges försvar och säkerhet. Vad

som är en personuppgift och behandling av personuppgifter definieras i 8 §.

I Försvarsmaktens uppgifter ingår att upprätthålla och utveckla ett militärt försvar som ytterst kan möta ett väpnat angrepp. Grunden för Försvarsmaktens verksamhet är förmågan till väpnad strid. Försvarsmakten ska försvara Sverige och främja svensk säkerhet samt upptäcka och avvisa kränkningar av det svenska territoriet. Försvarsmakten ska dessutom kunna värna Sveriges suveräna rättigheter och svenska intressen samt kunna förebygga och hantera konflikter och krig såväl nationellt som internationellt. Försvarsmakten ska kunna utföra dess uppgifter självständigt eller i samverkan med andra myndigheter, länder och organisationer. Vid höjd beredskap ska Försvarsmakten kunna krigsorganisera, mobilisera och använda alla krigsförband för att möta ett militärt hot mot Sverige och svenska intressen. Krigsförband ska kunna krigsorganiseras, även om höjd beredskap inte råder. Försvarsmaktens uppgifter utvecklas närmare i avsnitt 3.1.

De beskrivna uppgifterna ligger utanför unionsrätten. Även sådana arbetsuppgifter som kan tillkomma för Försvarsmaktens del, och som ligger utanför unionsrätten, ska behandlas med stöd av lagen.

3 §

Lagen gäller vid sådan behandling av personuppgifter som 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.

Paragrafen behandlas i avsnitt 6.2.4. Den begränsar lagens tillämpningsområde till sådan behandling av personuppgifter som 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.

4 §

Vid behandling av personuppgifter enligt denna lag gäller inte lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

Paragrafen behandlas i avsnitt 6.2.5. Den upplyser om att lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning inte gäller när personuppgifter behandlas enligt lagen om behandling av personuppgifter vid Försvarsmakten.

Förhållandet till annan reglering

5 §

Bestämmelserna i denna lag ska inte tillämpas i den utsträckning det skulle inskränka skyldigheten enligt 2 kap. tryckfrihetsförordningen att lämna ut personuppgifter.

Paragrafen, som behandlas i avsnitt 6.2.6, klargör att bestämmelserna i lagen inte ska tillämpas om det skulle inskränka Försvarsmaktens skyldighet enligt 2 kap. tryckfrihetsförordningen att lämna ut personuppgifter.

Personuppgiftsansvar

6 §

Försvarsmakten är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför.

Personuppgiftsansvaret omfattar all behandling av personuppgifter som utförs under myndighetens ledning eller på dess vägnar.

Bestämmelsen behandlas i avsnitt 6.2.7 och motsvarar 1 kap. 6 § lagen om behandling av personuppgifter vid Försvarets radioanstalt.

Personuppgiftsansvarig definieras i 1 kap. 8 § som den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter. Skyldigheterna som personuppgiftsansvarig regleras i 4 kap.

Bestämmelsen tydliggör att Försvarsmakten är personuppgiftsansvarig för all den personuppgiftsbehandling som myndigheten utför, dvs. även den behandling av personuppgifter som utförs under myndighetens ledning eller på dess vägnar.

Den närmare innebörden av personuppgiftsansvaret framgår av lagens övriga bestämmelser bl.a. att personuppgifter behandlas författningsenligt och på ett säkert sätt (4 kap. 1 och 4 §§) samt skyldigheter att tillgodose enskildas rättigheter (5 kap.) och behov av information vid tillsyn och kontroll (6 kap.).

Personuppgiftsansvaret omfattar all behandling av personuppgifter som utförs under den personuppgiftsansvariges ledning. Med det avses all personuppgiftsbehandling vid Försvarsmakten inom lagens verksamhetsområden. Det gäller både behandling som utförs genom en aktiv handling, t.ex. insamling eller sökning, och passiv behandling, t.ex. lagring.

Försvarsmakten är också ansvarig för all behandling av personuppgifter som utförs på dess vägnar. Med det avses främst sådan behandling som Försvarsmakten har uppdragit åt ett personuppgiftsbiträde att utföra. Försvarsmakten kan uppdra åt ett biträde att utföra viss behandling av personuppgifter, men kan inte genom det avsäga sig personuppgiftsansvaret. Bestämmelser om personuppgiftsbiträde finns i 4 kap. 7–11 §§.

7 §

Försvarsmakten får vara gemensamt personuppgiftsansvarig med annan endast i den utsträckning det följer av lag eller förordning eller om regeringen i ett enskilt fall beslutar om det.

Paragrafen behandlas i avsnitt 6.2.8. Gemensamt personuppgiftsansvar får endast förekomma om det har beslutats genom lag eller förordning eller av regeringen i ett enskilt fall. Försvarsmakten får inte på egen hand komma överens med en annan aktör om att personuppgiftsansvaret för viss personuppgiftsbehandling ska vara gemensamt.

Om det vid en bedömning av de faktiska omständigheterna konstateras att gemensamt personuppgiftsansvar föreligger, trots att det inte finns något beslut om det, står behandlingen i strid med denna paragraf.

Definitioner

8 §

I paragrafen, som behandlas i avsnitt 6.2.9, definieras vissa uttryck som används i lagen.

Behandling av personuppgifter

En åtgärd eller kombination av åtgärder som vidtas i fråga om personuppgifter eller uppsättningar av personuppgifter, oavsett om det görs automatiserat eller inte, t.ex. insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämnande, spridning eller tillhandahållande på annat sätt, justering, sammanföring, begränsning, radering eller förstöring.

Uttrycket behandling av personuppgifter omfattar alla åtgärder som vidtas med sådana uppgifter. Så snart personuppgifter hanteras på något sätt är det fråga om behandling som omfattas av lagens bestämmelser, om den är helt eller delvis automatiserad eller avser manuell behandling i en strukturerad samling av personuppgifter. Uppräkningen i definitionen av olika sätt att hantera personuppgifter är således inte uttömmande.

Biometriska uppgifter

Personuppgifter som rör en persons fysiska, fysiologiska eller beteendemässiga kännetecken, som tagits fram genom särskild teknisk behandling och som möjliggör eller bekräftar unik identifiering av personen i fråga.

Biometriska uppgifter behandlas i avsnitt 6.4.2. Biometri är ett samlingsnamn för sådan automatiserad teknik som syftar till att identifiera en person eller avgöra om en påstådd identitet är riktig. Den baseras på fysiska karaktärsdrag hos den som ska identifieras. Mönster av fingeravtryck, ansiktsgeometri, ögats iris, regnbågshinna och näthinna, röst, hand, blodkärl, dna eller gång är exempel på områden där sådan teknik kan användas. Gemensamt för teknikerna är att

kroppen mäts elektroniskt. Biometriska uppgifter är den information som kan tas fram ur ett biometriskt underlag. Uppgifterna kan användas för att skapa en referensmall eller för att jämföra med tidigare lagrade referensmallar i syfte att kontrollera en persons identitet. Fingeravtryck och dna-profiler är i dag de vanligaste formerna av biometriska uppgifter.

Biometriska uppgifter i form av fingeravtryck kan framgå av ett spår som påträffas vid utredning av en händelse som exempelvis ett angrepp mot svensk trupp utomlands. Även analys av spåren omfattas av definitionen, trots att de vid den tidpunkten inte går att härleda till en identifierad person. Dna-spår behandlas i kommentaren till uttrycket genetiska uppgifter.

Av 2 kap. 16 § framgår att biometriska uppgifter bara får behandlas om det är absolut nödvändigt för ändamålet med behandlingen.

Fotografier och filmer som inte bearbetas tekniskt i syfte att åstadkomma unik identifiering faller utanför definitionen. Bearbetning av bilder av personer för att förbättra bildkvaliteten, förstärka detaljer och liknande omfattas alltså inte. Om bilder däremot bearbetas i exempelvis ett ansiktsigenkänningsprogram i syfte att identifiera personer omfattas de av definitionen. Att fotografier kan omfattas av regleringen av känsliga personuppgifter på andra grunder behandlas i kommentaren till 2 kap. 15 §.

Dataskyddsombud

En fysisk person som utses av den personuppgiftsansvarige för att självständigt se till att personuppgifter behandlas författningsenligt och på ett korrekt sätt.

Dataskyddsombud behandlas i avsnitt 6.6.5.

Ett dataskyddsombud är en fysisk person som utses av den personuppgiftsansvarige att självständigt utföra vissa uppgifter i syfte att se till att personuppgifter behandlas författningsenligt och på ett korrekt sätt. Ett dataskyddsombud kan antingen vara anställd hos den personuppgiftsansvarige eller en utomstående. Kravet på självständighet innebär att dataskyddsombud ska kunna utföra sina arbetsuppgifter på ett oberoende sätt. Ombuden förutsätts framför allt ha

goda kunskaper om reglerna om personuppgiftsbehandling. Ombuden bör också ha sådan ställning i organisationen att deras synpunkter och råd tas på allvar.

Dataskyddsombudets uppgifter, som motsvarar personuppgiftsombudets uppgifter enligt 4 kap. 2–4 §§ FM-PuL, regleras i 4 kap. 6 §.

Genetiska uppgifter

Personuppgifter som rör en persons nedärvda eller förvärvade genetiska kännetecken och som härrör från analys av ett spår av eller ett prov från personen i fråga.

Genetiska uppgifter behandlas i avsnitt 6.4.2 och 6.4.4.

All information som rör en persons nedärvda eller förvärvade genetiska kännetecken och som kan tas fram ur ett spår från människokroppen omfattas av definitionen.

Genetiska uppgifter behandlas vid dna-analyser i forensisk verksamhet för att ta fram dna-profiler eller forensiska uppslag. Behandlingen kan avse genetiska uppgifter från såväl identifierade som oidentifierade personer. Eftersom nedärvda eller förvärvade genetiska kännetecken för en person kan framgå av ett spår som påträffas vid utredning av en händelse, omfattas även analys av spåren av definitionen, trots att de vid den tidpunkten inte går att härleda till en identifierad person. Själva dna-profilen, som behandlas i dna-register, utgör däremot inte en genetisk uppgift, eftersom inga nedärvda eller förvärvade genetiska kännetecken kan utläsas ur den. Dna-profilen är i stället en biometrisk uppgift, eftersom den tas fram genom en särskild teknisk behandling av en persons arvsmassa för att möjliggöra eller bekräfta unik identifiering av personen i fråga.

Logg

Behandlingshistorik som sparas viss tid.

Logg och logguppföljning behandlas i avsnitt 6.6.2.

En logg definieras som en behandlingshistorik som sparas viss tid.

Vad som ska loggas framgår av kommentaren till 4 kap. 2 §.

Mottagare

Den till vilken personuppgifter lämnas ut, med undantag av en myndighet som med stöd av författning utövar tillsyn, kontroll eller revision.

Mottagare definieras som den till vilken personuppgifter lämnas ut, med undantag av en myndighet som med stöd av författning utövar tillsyn, kontroll eller revision. Undantaget omfattar bl.a. myndigheter som tar del av personuppgifter i sin tillsyn och kontroll av viss verksamhet, t.ex. Datainspektionen och Statens inspektion för försvarsunderrättelseverksamheten. Även andra myndigheter som utövar tillsyn, t.ex. Riksdagens ombudsmän (JO) och Justitiekanslern, omfattas av undantaget.

Personuppgift

Varje upplysning om en identifierad eller identifierbar fysisk person som är i livet.

Med personuppgift avses varje upplysning om en identifierad eller identifierbar fysisk person som är i livet. Uttrycket behandlas i avsnitt 6.2.9.

Varje information som kan hänföras till en fysisk person är en personuppgift. Det gäller även information som kan hänföras till en individ om en fysisk person kan identifieras med hjälp av informationen. Det krävs inte att den personuppgiftsansvarige ska förfoga över samtliga uppgifter som gör identifieringen möjlig. Det innebär att t.ex. oidentifierade fingeravtryck och dna-profiler är personuppgifter, eftersom det är möjligt att identifiera en person med hjälp av dem. Även bild- eller ljudupptagningar kan utgöra personuppgifter, om man direkt eller indirekt kan avgöra vilken individ som upptagningen avser.

Definitionen omfattar bara uppgifter om personer som är i livet.

Uppgifter om juridiska personer omfattas inte av definitionen.

Personuppgiftsansvarig

Den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter.

Uttrycket behandlas i avsnitt 6.2.9.

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

Att bestämma ändamålen med behandlingen innebär i princip att bestämma att en behandling ska utföras och varför.

Att bestämma medlen för behandlingen avser främst att bestämma över de tekniska och organisatoriska medlen, dvs. hur behandlingen ska gå till. Det kan handla om vilka personuppgifter som ska behandlas, vilka som ska få ta del av dem och hur länge personuppgifterna får behandlas.

Den personuppgiftsansvarige styr dock inte alltid själv över alla medel för behandlingen. Vid direktåtkomst bestämmer den som medger åtkomsten hur tillgången tekniskt ska lösas och vilka personuppgifter som ska tillgängliggöras. Den som ges direktåtkomst är personuppgiftsansvarig för behandlingen av de personuppgifter som direktåtkomsten avser.

Personuppgiftsbiträde

Den som, med stöd av ett skriftligt avtal eller annan skriftlig överenskommelse, behandlar personuppgifter för den personuppgiftsansvariges räkning.

Uttrycket behandlas i avsnitt 6.2.9.

Ett personuppgiftsbiträde är en fysisk eller juridisk person som behandlar personuppgifter för den personuppgiftsansvariges räkning med stöd av ett skriftligt avtal eller en annan skriftlig överenskommelse. Kravet på att det ska finnas ett avtal eller en överenskommelse framgår av 4 kap. 8 §.

Ett personuppgiftsbiträde behandlar personuppgifter endast enligt instruktioner från den personuppgiftsansvarige och har inte rätt att själv bestämma över personuppgiftsbehandlingen. Ett personuppgiftsbiträde finns alltid utanför den egna organisationen En anställd eller

någon annan som behandlar personuppgifter under den personuppgiftsansvariges direkta ansvar kan inte vara personuppgiftsbiträde.

Tredje part

Någon annan än den som personuppgiften rör, personuppgiftsansvarige, dataskyddsombudet, personuppgiftsbiträdet och sådana personer som under den personuppgiftsansvariges eller personuppgiftsbiträdets direkta ansvar har rätt att behandla personuppgifter.

Uttrycket behandlas i avsnitt 6.2.9.

Uppgiftssamling

En samling med uppgifter som med hjälp av automatiserad behandling är gemensamt tillgängliga.

Uppgiftssamlingar behandlas i avsnitt 6.5.

Avgörande för när automatiserat behandlade uppgifter ska anses ingå i en uppgiftssamling är att uppgifterna är gemensamt tillgängliga i en viss verksamhet för de ändamål som ska styra behandlingen av uppgifter inom verksamheten.

2 kap. Behandling av personuppgifter

Rättsliga grunder

Försvar och säkerhet

1 §

Försvarsmakten får behandla personuppgifter om det är nödvändigt för att planera, förbereda och genomföra verksamhet som rör

1. Sveriges försvar och säkerhet, eller

2. internationellt försvars- och säkerhetssamarbete.

Försvarsmaktens uppgift att bedriva verksamhet som anges i första stycket ska följa av lag, förordning eller ett särskilt beslut i vilket regeringen uppdragit åt myndigheten att utföra uppgiften.

Paragrafen anger Sveriges försvar och säkerhet som en rättslig grund för Försvarsmaktens personuppgiftsbehandling. Ämnet behandlas i avsnitt 6.3.1.

Personuppgifter får enligt *första stycket* behandlas av Försvarsmakten om det är nödvändigt för att planera, förbereda och genomföra viss verksamhet. Bestämmelsen bildar den yttre ramen för när behandling av personuppgifter är tillåten.

Enligt *första stycket punkten 1* får personuppgifter behandlas om det är nödvändigt för att planera, förbereda och genomföra verksamhet som rör Sveriges försvar och säkerhet. Försvarsmaktens uppgift att bedriva sådan verksamhet ska framgå av lag, förordning eller ett särskilt beslut i vilket regeringen uppdragit åt myndigheten att ansvara för uppgiften. Exempel på sådana uppgifter anges i avsnitt 6.3.1.

Som framgår av avsnitt 6.3.1 är beskrivningen av verksamheterna är inte fullständig. Det kan finnas andra uppgifter för Försvarsmakten som rör Sveriges försvar och säkerhet och nya uppgifter kan tillkomma.

I avsnitt 6.3.1 ges exempel på författningsenliga uppgifter som faller utanför bestämmelsen.

Enligt *första stycket punkten 2* får personuppgifter behandlas om det är nödvändigt för att planera, förbereda och genomföra verksamhet som rör internationellt försvars- och säkerhetssamarbete.

Enligt *andra stycket* ska Försvarsmaktens uppgifter att bedriva verksamhet enligt första stycket framgå av lag, förordning eller ett särskilt beslut i vilket regeringen uppdragit åt myndigheten att ansvara för uppgiften. Exempel på sådana uppgifter redovisas i avsnitt 6.3.1.

En närmare beskrivning av Försvarsmaktens internationella samarbeten finns i avsnitt 3.1. Myndighetens deltagande i sådana samarbeten sker med stöd av regeringens beslut.

Särskilt om försvarsunderrättelseverksamhet

2 §

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

Paragrafen behandlas i avsnitt 6.3.2. och anger de ändamål för vilka personuppgifter får användas i försvarsunderrättelseverksamheten genom en hänvisning till lagen (2000:130) om försvarsunderrättelseverksamhet.

Försvarsunderrättelseverksamheten är ett led i Försvarsmaktens uppgifter att i fred, under beredskap och i krig ge underlag för Försvarsmaktens 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 inriktningen av försvarsunderrättelseverksamheten.

Försvarsunderrättelseverksamheten ska 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.

I underrättelseverksamhetens natur ligger att det inte går att på förhand göra tydliga avgränsningar av vilka uppgifter som måste inhämtas för att nå det slutliga målet att åstadkomma de underrättelser som uppdragsgivarna efterfrågar. Inhämtad information kan motivera inhämtning av annan information som man från början inte kände till. Det kan också uppkomma behov av att värdera trovärdigheten hos källor, som man heller inte kände till från början. Verksamheten kan också gå ut på att leta efter företeelser och hot som är okända men som antas existera.

3 §

De personuppgifter som Försvarsmakten har fått tillgång till i myndighetens försvarsunderrättelseverksamhet får fortsatt behandlas i den verksamheten, om det behövs för att fullgöra den.

Vad som sägs i första stycket gäller endast om inget annat följer av denna lag eller förordning som regeringen har meddelat i anslutning till lagen.

Paragrafen behandlas i avsnitt 6.3.2 och innebär en komplettering av ändamålsbeskrivningen i 2 § på så sätt att de personuppgifter som

Försvarsmakten har fått tillgång till i sin försvarsunderrättelseverksamhet även fortsättningsvis får behandlas i den verksamheten, om det behövs för att fullgöra den.

En förutsättning för behandlingen enligt bestämmelsen är att den inte strider mot någon annan bestämmelse i lagen eller tillhörande förordning. Detta tydliggörs i *andra stycket*.

Särskilt om militär säkerhetstjänst

4 §

Personuppgifter får behandlas i Försvarsmaktens militära säkerhetstjänst för att upptäcka, förebygga och avvärja säkerhetshotande verksamhet som riktas mot Försvarsmakten och dess säkerhetsintressen, om det är nödvändigt för att

1. klarlägga verksamhet som innefattar hot mot Sveriges säkerhet, eller

2. vidta åtgärder som hindrar eller försvårar säkerhetshotande verksamhet.

Paragrafen, som behandlas i avsnitt 6.3.3, anger de ändamål för vilka uppgifter får behandlas i den militära säkerhetstjänsten.

Ändamålet med behandlingen av personuppgifter inom den militära säkerhetstjänsten är att tjänsten ska kunna fullgöra de uppgifter som följer av säkerhetsskyddslagen (1996:627), säkerhetsskyddsförordningen (1996:633) och förordningen (2007:1266) 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 5 § också behandlas uppgifter om personer med anknytning till sådan verksamhet. Med denna punkt avses säkerhetsunderrättelsetjänst. Verksamheten sker i stort under samma arbetsformer och med utnyttjande av samma typ av källor som används i försvarsunderrättelseverksamheten.

Inom säkerhetsskyddstjänsten, som avses i *punkten 2*, vidtas olika åtgärder för att förhindra eller försvåra säkerhetshotande verksamhet. Verksamheten består i 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.

Punkten 2 omfattar också signalskyddstjänst, som syftar till att minska verkan av signalspaning, falsk signalering och störsändning mot totalförsvarets telekommunikations- och informationssystem. Verksamheten ska förhindra obehörig insyn i och påverkan av totalförsvarets telekommunikationer, samt verka för 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 stickprovsvis med hjälp av fasta eller rörliga kontrollorgan. I 7 § finns en särskild bestämmelse om personuppgiftsbehandling i signalkontrollverksamheten.

5 §

Uppgifter om en person får behandlas för det ändamål som anges i 4 § endast om

1. uppgifterna är nödvändiga för att kartlägga verksamhet som innefattar brott som kan hota Sveriges säkerhet eller terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott eller motsvarande brottslighet enligt tidigare lagstiftning,

2. uppgifterna är nödvändiga för att kartlägga underrättelseverksamhet riktad mot Försvarsmakten och dess säkerhetsintressen,

3. uppgifterna är nödvändiga för att kartlägga annan säkerhetshotande verksamhet än som avses i 1 och som innefattar brott eller åsidosättande av åligganden i anställning hos Försvarsmakten, och det finns särskilda skäl till att uppgiften ska 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 säkerhetsprövning enligt säkerhetsskyddslagen (1996:627) eller i annat fall är nödvändiga för att hantera en uppgift som rör säkerhetsskydd.

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. En närmare beskrivning av de fem punkterna finns i avsnitt 6.3.3.

6 §

Personuppgifter som behandlas enligt 5 § ska förses med upplysning om på vilken av de angivna grunderna uppgiften behandlas. Om behandlingen av en personuppgift föranleds av något annat än antagande om att personen har utövat eller kommer att utöva brottslig verksamhet ska 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 ska förses med en särskild upplysning om detta, om det inte på annat sätt klart framgår att sådant antagande inte finns.

Personuppgifter som behandlas enligt 5 § första stycket 1–3 ska i förekommande fall förses med en upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak.

Bestämmelsen behandlas i avsnitt 6.3.3.

När uppgifter behandlas i den militära säkerhetstjänsten är det av integritetsskäl viktigt att särskilja olika typer av uppgifter. Särskilt viktigt är att det inte uppstår missuppfattningar om någon kan antas faktiskt utöva eller förbereda säkerhetshotande verksamhet eller inte. I *första stycket* anges att uppgifter om en person ska förses 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 ska detta särskilt anges, om det inte klart framgår på annat sätt. På motsvarande sätt ska anges

om det inte heller kan antas att personen bedriver säkerhetshotande verksamhet som inte utgör brott. Utgångspunkten är 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 *andra stycket* föreskrivs att uppgifter om att en person som avses i punkterna 1–3 ska förses med upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. Detta innebär att en särskild upplysning i förekommande fall ska lämnas om vilken trovärdighet som tillmäts t.ex. den som lämnat ett tips till säkerhetstjänsten. Om möjligt ska också anges hur korrekt uppgiften är, t.ex. om det är en obekräftad gissning eller ett belagt faktum.

7 §

Trots vad som sägs i 5 och 6 §§ får personuppgifter som ingår i eller har uppkommit i samband med användning av totalförsvarets telekommunikations- och informationssystem behandlas för att förhindra obehörig insyn i och påverkan av dessa system. Det gäller även sådana uppgifter som avses i 15, 16, 18 och 19 §§. Behandling som särskilt syftar till att identifiera en person får dock endast utföras om bestämmelserna i 5 § första stycket 1, 2 eller 3 tillämpas.

Bestämmelsen, som behandlas i avsnitt 6.3.3, 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 5 § första stycket 1, 2 eller 3.

Övriga rättsliga grunder

8 §

Personuppgifter som utgör allmänt tillgänglig information får behandlas av Försvarsmakten om det är nödvändigt för de ändamål som anges i 1, 2 och 4 §§.

Bestämmelsen behandlas i avsnitt 6.3.4.

För att kunna bedriva en effektiv försvarsunderrättelseverksamhet behöver Försvarsmakten, utöver den information som den inhämtar genom hemliga metoder, också ha god tillgång till allmänt tillgänglig information. Därigenom kan den på hemligt sätt inhämtade informationen på ett bättre sätt än eljest sättas in i sitt rätta sammanhang. Av intresse här är information som utgörs av personuppgifter som kan påträffas vid sökning på internet eller vid sökningar i öppna databaser. Uppgifterna kan vara gratis eller tillgängliga på kommersiell grund. Gemensamt för dem är att de är publikt tillgängliga. Det kan röra sig om uppgifter som t.ex. en abonnent på ett eller annat sätt har samtyckt att uppgifterna finns med i elektroniska telefonkataloger eller förteckningar över ip-adresser i olika länder. I stället för att myndigheten exponerar sig kan databaserna anskaffas och läggas upp som referensdatabaser hos myndigheten där den kan göra sökningar.

Bestämmelsen gör det också möjligt att behandla personuppgifter på det beskrivna sättet när det gäller planering, förberedelse och genomförande av verksamhet som avser Sveriges försvar och säkerhet eller internationellt försvars- och säkerhetssamarbete liksom när det gäller verksamhet inom den militära säkerhetstjänsten.

9 §

Personuppgifter får behandlas av Försvarsmakten om det är nödvändigt för diarieföring, arkivering, handläggning av ett ärende eller för att utföra annan liknande uppgift som åligger myndigheten.

Bestämmelsen behandlas i avsnitt 6.3.5.

Genom bestämmelsen har den behandling av personuppgifter som uppkommer i de i avsnittet beskrivna verksamheterna direkt stöd i lag.

10 §

Försvarsmakten får behandla personuppgifter för vetenskapliga, statistiska eller historiska ändamål inom denna lags tillämpningsområde.

Bestämmelsen behandlas i avsnitt 6.3.10.

Genom bestämmelsen ges Försvarsmakten möjlighet att behandla personuppgifter för historiska, statistiska eller vetenskapliga ändamål.

11 §

Försvarsmakten får behandla personuppgifter för att kunna tillgodose enskildas behov av information enligt 5 kap. och kunna lämna information vid tillsyn eller kontroll.

Bestämmelsen behandlas i avsnitt 6.3.11.

Datainspektionen är tillsynsmyndighet för Försvarsmaktens personuppgiftsbehandling. Även Statens inspektion för försvarsunderrättelseverksamheten (Siun) har till uppgift att kontrollera försvarsunderrättelseverksamheten hos de myndigheter som bedriver sådan verksamhet, däribland vilka personuppgifter som behandlas i denna verksamhet. Sökningar i uppgiftssamlingar och sammanställningar av uppgifter som är nödvändig för att Försvarsmakten ska kunna tillmötesgå tillsynsmyndighetens och kontrollmyndighetens behov innebär att personuppgifter behandlas. Bestämmelsen utgör rättslig grund för denna personuppgiftsbehandling samt för den personuppgiftsbehandling som krävs för att tillmötesgå enskildas rätt till information enligt 5 kap. Enskildas rättigheter behandlas vidare i avsnitt 6.7.2. Tillsynsmyndighetens verksamhet behandlas i avsnitt 6.8.

Bestämmelsen utgör även den rättsliga grunden för personuppgiftshantering i Försvarsmaktens loggfunktioner för de syften som framgår av denna bestämmelse. Bestämmelser om myndigheternas loggfunktioner behandlas vidare i avsnitt 6.6.2.

Grundläggande krav

Ändamål

12 §

Personuppgifter får bara behandlas för särskilda, uttryckligt angivna och berättigade ändamål.

Personuppgifter får inte behandlas för något ändamål som är oförenligt med det ändamål för vilket personuppgifterna ursprungligen behandlades.

Bestämmelsen behandlas i avsnitt 6.4.1.

Paragrafen sätter, tillsammans med bestämmelserna i 13 och 14 §§, vissa ramar för Försvarsmaktens personuppgiftsbehandling inom lagens verksamhetsområden.

Bestämmelsen ställer i *första stycket* krav på att varje personuppgiftsbehandling ska ha koppling till de ändamål som anges i lagen, dvs. vara relevant i de verksamheter som utgör rättsliga grunder för personuppgiftsbehandling och är ägnade att lösa Försvarsmaktens uppgifter enligt lag eller annan författning. Detta innebär att ändamålen med en behandling av personuppgifter måste bestämmas redan när uppgifterna samlas in.

Paragrafens *andra stycke* ger uttryck för den generella s.k. finalitetsprincipen, dvs. att fortsatt behandling av personuppgifter inte få ske för något ändamål som är oförenligt med det ändamål för vilket personuppgifterna ursprungligen behandlades. Vad som ska anses vara oförenliga ändamål måste avgöras från fall till fall, men de ändamål som anges i lagen är att betrakta som förenliga för fortsatt behandling. Den innebär att den personuppgiftsansvarige under hela behandlingstiden måste hålla reda på för vilka ändamål varje personuppgift har samlats in. Se prop. 2006/07:46 s. 56 f.

Författningsenlig och korrekt behandling

13 §

Personuppgifter ska behandlas författningsenligt och på ett korrekt sätt.

Paragrafen behandlas i avsnitt 6.4.1.

Personuppgifter får enligt bestämmelsen bara behandlas om det är författningsenligt, dvs. enligt lag eller annan författning.

Vad som är ett korrekt sätt för behandling styrs emellertid inte bara av bestämmelser i författning och den praxis som utbildas kring dem. Tillsynsmyndighetens allmänna råd och uttalanden i fråga om personuppgiftsbehandling har också betydelse, liksom myndigheternas interna regler.

Personuppgifternas kvalitet

14 §

Personuppgifter som behandlas ska vara adekvata och relevanta i förhållande till ändamålen med behandlingen och, om det är nödvändigt, uppdaterade.

Uppgifter som beskriver en persons utseende ska utformas på ett objektivt sätt med respekt för människovärdet.

Fler personuppgifter får inte behandlas än vad som är nödvändigt med hänsyn till ändamålen med behandlingen.

Paragrafen behandlas i avsnitt 6.4.1.

Enligt *första stycket* ska de behandlade uppgifterna vara adekvata och relevanta i förhållande till ändamålet med behandlingen. Detta innebär bl.a. att ovidkommande uppgifter inte får behandlas. En prövning av om en personuppgift är nödvändig för behandlingen ska göras kontinuerligt av den behöriga myndigheten, inte bara när uppgiften registreras eller på annat sätt samlas in. Även vid en senare behandling ska personuppgiften behövas för just den behandlingen, annars är kravet på adekvans och relevans inte uppfyllt. De personuppgifter som behandlas behöver vara uppdaterade, om det är nödvändigt. Frågan om det är nödvändigt att de är uppdaterade får avgöras med hänsyn till ändamålen med behandlingen.

Enligt *andra stycket* ska uppgifter som beskriver en persons utseende ska utformas på ett objektivt sätt med respekt för människovärdet. Syftet med bestämmelsen är att förhindra att personers utseende beskrivs i ordalag som kan vara kränkande för individen.

Utformningen av bestämmelsen innebär att myndigheten alltid är oförhindrad att, när den får ett tips från allmänheten eller en samarbetspartner om en person som kan misstänkas för verksamhet som exempelvis innebär säkerhetshot mot Försvarsmaktens intressen, göra de anteckningar som är nödvändiga för att underlätta identifieringen av personen, t.ex. anteckningar om fysiska kännetecken. Anteckningarna måste dock utformas på ett objektivt sätt. I anslutning till dessa anteckningar får även sådana känsliga personuppgifter som avses i 15 § antecknas, om det är absolut nödvändigt för det arbete som tipset bör föranleda.

Enligt *tredje stycket* får inte fler personuppgifter behandlas än vad som är nödvändigt med hänsyn till ändamålen med behandlingen. Vad som utgör nödvändig behandling får avgöras av den personuppgiftsansvarige vid varje behandling. Att uppgifterna inte får vara fler än nödvändigt understryker kravet på att en fortlöpande bedömning görs.

Sammantaget måste det vid all behandling prövas om det går att utelämna personuppgifter, eller i vart fall att endast använda uppgifter som indirekt går att hänföra till en viss person. Om fullständig avidentifiering är ett fullgott alternativ till att använda direkta eller indirekta personuppgifter är förutsättningarna för att behandla personuppgifterna inte uppfyllda.

Känsliga personuppgifter

15 §

Personuppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening eller som rör hälsa, sexualliv eller sexuell läggning får inte behandlas.

När uppgifter om en person behandlas får de dock kompletteras med sådana uppgifter som avses i första stycket, om det är absolut nödvändigt för syftet med behandlingen.

Paragrafen reglerar tillsammans med 16 och 17 §§ i vilken utsträckning känsliga personuppgifter får behandlas. Att uppgifterna betecknas som känsliga personuppgifter framgår av rubriken. Paragrafen behandlas i avsnitt 6.4.2.

Enligt *första stycket* får personuppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening eller som rör hälsa, sexualliv eller sexuell läggning inte behandlas. Det innebär att det inte är tillåtet att föra register över eller på annat sätt göra anteckningar om enskilda på den grunden att de utifrån etniskt ursprung, politiska åsikter eller något annat i paragrafen angivet förhållande kan hänföras till en viss kategori av människor.

En uppgift om utseende är normalt inte en känslig personuppgift och den får alltså behandlas, med den begränsning som följer av 14 § andra stycket. Om en sådan uppgift samtidigt innebär uppgift om etniskt ursprung omfattas den dock av förbudet. Bestämmelsen hindrar inte att uppgifter om en persons nationalitet behandlas, eftersom en sådan uppgift normalt inte ger upplysning om etniskt ursprung (se prop. 2009/10:85 s. 325). Uppgifter om att en viss person kommer från en viss världsdel eller ett visst land faller också som regel utanför förbudet mot behandling av känsliga personuppgifter. Skulle en sådan personuppgift i det enskilda fallet t.ex. avslöja etniskt ursprung är dock förbudet tillämpligt.

I *andra stycket* görs undantag från huvudregeln att känsliga personuppgifter inte får behandlas. Uppgifter om en person som behandlas på annan grund får kompletteras med känsliga personuppgifter, om det är absolut nödvändigt för ändamålet med behandlingen. Det innebär att om andra uppgifter om en person samlas in får de kompletteras med uppgifter om exempelvis religiös övertygelse eller etniskt ursprung om det är av stor betydelse för syftet med behandlingen. Med hänsyn till den restriktivitet som ligger i uttrycket ”absolut nödvändigt” måste dock behovet av att göra sådana kompletteringar prövas noga i det enskilda fallet.

Känsliga personuppgifter kan också förekomma i Försvarsmaktens verksamhet på grund av att någon har lämnat en sådan uppgift i ett tips eller förhör. Det kan vara fråga om helt grundlösa påståenden. Eftersom Försvarsmakten inte kan hindra någon från att yttra sig

vare sig muntligen eller skriftligen på dessa sätt, kan känsliga personuppgifter komma att behandlas. Behandlingen av den känsliga personuppgiften omfattas i dessa fall av undantaget i andra stycket.

16 §

Biometriska uppgifter får behandlas endast om det är absolut nödvändigt för ändamålet för behandlingen. Genetiska uppgifter får inte behandlas.

Paragrafen reglerar i vilken utsträckning biometriska uppgifter får behandlas. Paragrafen behandlas i avsnitt 6.4.2.

Med biometriska uppgifter avses enligt definitionen i 1 kap. 8 § personuppgifter som rör en fysisk persons fysiska, fysiologiska eller beteendemässiga kännetecken som tagits fram genom särskild teknisk behandling och som möjliggör eller bekräftar unik identifiering av personen i fråga.

Bestämmelsen möjliggör användning av särskild teknisk behandling för att bekräfta unik identifiering av en person. Det innebär att t.ex. fingeravtryck, ansiktsgeometri, röstigenkänning eller rörelsemönster kan användas för att identifiera en person. Behovet av att behandla biometriska uppgifter måste prövas noga i ett enskilt ärende.

Försvarsmakten får inte behandla genetiska uppgifter. Uttrycket definieras i 1 kap. 8 §.

17 §

Vid sökning får personuppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening eller som rör hälsa, sexualliv eller sexuell läggning användas som sökbegrepp om det är absolut nödvändigt för syftet med behandlingen. Detsamma gäller biometriska uppgifter.

Paragrafen reglerar i vilken utsträckning känsliga personuppgifter får användas som sökbegrepp. Paragrafen behandlas i avsnitt 6.4.2.

Paragrafen gäller generellt, dvs. såväl personuppgifter som har gjorts gemensamt tillgängliga som personuppgifter som inte har det.

Bestämmelsen gör det möjligt att utföra sökning i syfte att få fram ett personurval grundat på känsliga personuppgifter, t.ex. i

syfte att få fram ett urval av personer som t.ex. har viss politisk åskådning eller religiös övertygelse etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller uppgifter som rör hälsa, sexualliv eller sexuell läggning, om sökningen är *absolut nödvändig* för de syften som utgör rättslig grund för Försvarsmaktens personuppgiftsbehandlingar. Försvarsmakten kan behöva söka på uppgifter som rör politiska åsikter, religiös övertygelse eller etniskt ursprung, eftersom det ingår i Försvarsmaktens uppdrag att kartlägga sådan verksamhet som kan komma att hota Sveriges försvar och säkerhet. Sådan sökning kan även behöva göras t.ex. för att förebygga, förhindra eller utreda angrepp mot svensk personal vid insatser utomlands. Kravet på att det ska vara absolut nödvändigt att göra sökningen gör att utrymmet för sådana sökningar är begränsat och att rutinmässiga sökningar på känsliga uppgifter inte är tillåtna.

I vilken utsträckning det är tillåtet att behandla någon eller några av personuppgifterna i en sammanställning av sådana uppgifter som sökningen resulterat i får prövas mot huvudregeln om behandling av känsliga personuppgifter i 15 §. Rätten att göra sökning medför således inte en generell rätt att fortsätta att behandla uppgifterna.

Personnummer

18 §

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

1. ändamålet med behandlingen,
2. vikten av en säker identifiering, eller
3. något annat beaktansvärt skäl.

Paragrafen reglerar i vilken omfattning personnummer får behandlas vid Försvarsmakten. Paragrafen behandlas i avsnitt 6.4.3.

Om den som uppgifterna rör har offentliggjort uppgifterna eller lämnat sitt samtycke

19 §

Utan hinder av vad som föreskrivs i 15, 16 och 18 §§ får personuppgifter behandlas, om den som personuppgifterna rör har lämnat sitt uttryckliga samtycke eller på ett tydligt sätt har offentliggjort uppgifterna.

Första stycket gäller inte genetiska uppgifter.

Paragrafen behandlas i avsnitt 6.4.4.

Paragrafen ger Försvarsmakten möjlighet att behandla känsliga personuppgifter, om den som personuppgifterna rör har lämnat sitt uttryckliga samtycke eller på ett tydligt sätt har offentliggjort uppgifterna. Samtyckessituationer kan exempelvis förekomma i Försvarsmaktens militära säkerhetstjänst vid säkerhetsprövningar. Paragrafen ger även Försvarsmakten möjlighet att behandla personuppgifter som tydligt har offentliggjorts genom att de exempelvis tillkännagetts på internet.

Bestämmelsen gäller inte genetiska uppgifter.

Behandling av personuppgifter i vissa fall

20 §

Hantering av information som innebär behandling av personuppgifter ska inte anses oförenlig med bestämmelserna i 1, 2, 4, 5, 7, 8 och 12–16 §§ i det skede av behandlingen då det inte har kunnat fastställas vilka personuppgifter som informationen innehåller.

Paragrafen behandlas i avsnitt 6.4.5.

Bestämmelsen innebär att hantering av information som innebär behandling av personuppgifter inte ska anses oförenlig med bestämmelserna om tillåtlighet, ändamål, författningsenlig och korrekt behandling, personuppgifternas kvalitet och känsliga personuppgifter i det skede av behandlingen då det ännu inte har kunnat fastställas vilka personuppgifter som informationen innehåller.

När det står klart att informationen innehåller personuppgifter, samt vilka personuppgifterna är, ska Försvarsmakten behandla personuppgifterna enligt övriga bestämmelser i lagen.

Längsta tid som personuppgifter får behandlas

21 §

Personuppgifter som behandlas automatiserat får inte behandlas under längre tid än vad som behövs för något eller några av de ändamål som anges i 1–11 §§.

Regeringen eller den myndighet regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter eller i ett enskilt fall besluta att personuppgifter får behandlas under endast viss tid eller bevaras för historiska, statistiska eller vetenskapliga ändamål.

Paragrafen, som behandlas i avsnitt 6.4.6, innehåller en generell bestämmelse om hur länge Försvarsmakten får behandla personuppgifter.

Enligt *första stycket* får personuppgifter som behandlas automatiserat enligt bestämmelsen inte behandlas under längre tid än vad som behövs för något eller några av de ändamål för vilka Försvarsmakten får behandla personuppgifter (1–11 §§). Det som avses är ändamålet i det enskilda fallet. Ibland behandlas personuppgifter för flera olika ändamål. Att det inte längre finns behov av att behandla personuppgiften för ett visst ändamål medför inte att behandlingen av den måste upphöra för alla andra ändamål samtidigt. Å andra sidan innebär det förhållandet att personuppgiften fortfarande behövs för ett visst ändamål inte att den får fortsätta att behandlas för alla ändamål lika länge. Finns det inte längre behov av att behandla uppgifterna för något av ändamålen får de bara behandlas för arkivändamål. Behovet av att fortsätta att behandla uppgifterna måste därför prövas kontinuerligt. Om det är tillräckligt att behandla avidentifierade uppgifter är det inte längre tillåtet att behandla personuppgifterna.

Bestämmelsen ger även stöd för fortsatt behandling av personuppgifter i ett avslutat ärende om uppgifterna bedöms ha ett allmänt värde för exempelvis Försvarsmaktens försvarsunderrättelseverksamhet eller militära säkerhetstjänst. En grundläggande förutsättning för fortsatt behandling är att Försvarsmakten bedömer att uppgifterna behöver finnas tillgängliga ytterligare en viss tid för något av de ändamål för vilka Försvarsmakten får behandla personuppgifter. När det gäller ostrukturerad underrättelseinformation kan det vara särskilt svårt att bedöma det fortsatta behovet av behandling. Bedömningen måste innan bearbetningen är genomförd göras på ett

mer övergripande plan och i större utsträckning utgå från sannolikheten av att personuppgifterna kan komma att behövas i verksamheten än en reell bedömning av den enskilda uppgiften.

Bestämmelsen hindrar inte att Försvarsmakten med stöd i annan författning arkiverar och bevarar allmänna handlingar eller att arkivmaterial lämnas till en arkivmyndighet.

I *andra stycket* finns en upplysningsföreskrift om att regeringen eller den myndighet regeringen bestämmer kan meddela föreskrifter eller i ett enskilt fall besluta att personuppgifter får behandlas endast under viss tid eller bevaras för historiska, statistiska eller vetenskapliga ändamål.

Utlämnande av personuppgifter

22 §

Personuppgifter som behandlas med stöd av denna lag får föras över till andra länder eller internationella organisationer endast om sekretess inte hindrar det och det är nödvändigt för att Försvarsmakten ska kunna fullgöra sina uppgifter inom ramen för internationellt försvars- och säkerhetssamarbete.

Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter eller i enskilt fall besluta att överföring får ske även i andra fall om det är nödvändigt för verksamheten vid Försvarsmakten.

Enligt paragrafen, som behandlas i avsnitt 6.4.7, får personuppgifter föras över till andra länder eller internationella organisationer endast om sekretess inte hindrar det och det är nödvändigt för att Försvarsmakten ska 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 utlämnande ska ske eller inte måste i sin helhet avgöras efter en sekretessprövning och försvars- och säkerhetspolitiska överväganden.

Av bestämmelsen framgår vidare att begränsningarna av möjligheterna till överföring gäller såvida inte regeringen har meddelat föreskrifter eller beslut i enskilda fall om att överföring får ske även

i andra fall då det är nödvändigt för verksamheten vid Försvarsmakten.

23 §

Personuppgifter får lämnas ut elektroniskt på annat sätt än genom direktåtkomst, om det inte är olämpligt.

Elektroniskt utlämnande genom direktåtkomst är tillåtet bara i den utsträckning som anges i 3 kap. 2–4 §§.

Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om begränsning av möjligheten att lämna ut personuppgifter elektroniskt enligt första stycket.

Paragrafen, som behandlas i avsnitt 6.4.7, reglerar elektroniskt utlämnande.

Bestämmelsens *första stycke* innebär att en större mängd personuppgifter kan lämnas ut elektroniskt, om det inte är olämpligt.

I princip anses allt elektroniskt utlämnande som inte görs genom direktåtkomst utlämnat på medium för automatiserad behandling. Sådant utlämnande kan göras på många olika sätt. Det kan vara fråga om att personuppgifter lämnas t.ex. via e-post eller dvd-skiva eller genom direkt överföring från ett datasystem till ett annat via elektroniska kommunikationsnät.

Det har betydelse vem mottagaren är för frågan om det är olämpligt att lämna ut uppgifter elektroniskt. Som regel kan det inte anses vara olämpligt att lämna ut uppgifter på det sättet till en myndighet (se prop. 2014/15:148 s. 113, jfr SOU 2015:39 s. 447 f.).

När det gäller utlämnande till andra än svenska myndigheter krävs en mer nyanserad bedömning med hänsyn till bl.a. innehållet i handlingen och vem (t.ex. en organisation) som är mottagare. Bedömer myndigheten att det finns risk för att personuppgifterna kan komma att missbrukas om de lämnas ut elektroniskt kan det var olämpligt att lämna ut dem på detta sätt. Vid prövningen av om personuppgifter bör lämnas ut elektroniskt bör även informationssäkerheten, dvs. säkerheten hos mottagaren, vägas in.

Andra stycket anger att elektroniskt utlämnande genom direktåtkomst endast är tillåtet bara i den utsträckning som särskilt anges i lagen (3 kap. 2–4 §§).

Tredje stycket upplyser om att regeringen kan meddela föreskrifter som begränsar möjligheten att lämna ut personuppgifter elektroniskt på annat sätt än genom direktåtkomst.

3 kap. Gemensamt tillgängliga uppgifter

Personuppgifter som får göras gemensamt tillgängliga

1 §

Personuppgifter får göras gemensamt tillgängliga om det behövs för något av de ändamål som anges i 2 kap. Personuppgifter som endast ett fåtal personer har tillgång till anses inte som gemensamt tillgängliga.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter eller besluta i enskilda fall vilka uppgiftssamlingar som får finnas och vilka uppgifter som får behandlas i respektive uppgiftssamling.

I paragrafen anges genom en hänvisning till lagens syften vilka personuppgifter som får göras gemensamt tillgängliga. Paragrafen behandlas i avsnitt 6.5.1.

En grundläggande förutsättning för att personuppgifter ska anses vara gemensamt tillgängliga är att de kan användas gemensamt av flera, dvs. att fler än en person har åtkomst till uppgifterna. Uppgifter som endast ett fåtal personer har rätt att ta del av bör dock inte anses som gemensamt tillgängliga.

Av *andra stycket* framgår att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter eller besluta i enskilda fall vilka uppgiftssamlingar som får finnas och vilka uppgifter som får behandlas i respektive uppgiftssamling.

Direktåtkomst

Försvarsunderrättelseverksamhet

2 §

Trots sekretess enligt 38 kap. 4 § offentlighets- och sekretesslagen (2009:400) får Säkerhetspolisen och Försvarets radioanstalt medges direktåtkomst till personuppgifter som utgör bearbetningsunderlag och analysresultat inom försvarsunderrättelseverksamheten och som finns i uppgiftssamlingar.

I paragrafen anges vilka myndigheter som får medges direktåtkomst till uppgifter som har gjorts gemensamt tillgängliga i uppgiftssamlingar och för vilka syften. Paragrafen behandlas i avsnitt 6.5.2.

Bestämmelserna om sekretess till skydd för enskilda i försvarsunderrättelsemyndigheternas verksamhet finns bl.a. i 38 kap. 4 § offentlighets- och sekretesslagen (2009:400). Sekretess gäller för uppgift om en enskilds personliga och ekonomiska förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till honom eller henne lider skada eller men (omvänt skaderekvisit). Bestämmelsen om direktåtkomst innebär att sådana uppgifter som anges i sekretessbestämmelsen får lämnas till Säkerhetspolisen och Försvarets radioanstalt genom direktåtkomst.

Bearbetningsunderlag och analysresultat består av information som ännu inte har bearbetats till underrättelserapporter.

3 §

Om det behövs för samarbetet mot terrorism eller vid svenskt deltagande i annat internationellt underrättelse- och säkerhetssamarbete får, i den utsträckning det följer av lag eller förordning eller om regeringen i ett enskilt fall beslutat om det, en utländsk underrättelse- eller säkerhetstjänst medges direktåtkomst till personuppgifter som behandlas med stöd av 2 kap. 2 § och som finns i uppgiftssamlingar.

I paragrafen regleras Försvarsmaktens möjlighet att medge utländsk underrättelse- och säkerhetstjänst direktåtkomst till vissa personuppgifter. Paragrafen behandlas i avsnitt 6.5.2.

Möjligheten att dela information genom direktåtkomst begränsas till underrättelse- och säkerhetstjänster. Underrättelse- och säkerhetstjänsterna får endast medges direktåtkomst om det behövs för samarbetet mot terrorism eller vid svenskt deltagande i annat internationellt underrättelse- och säkerhetssamarbete. Direktåtkomst får endast medges till personuppgifter som behandlas i Försvarsmaktens försvarsunderrättelseverksamhet och som finns i uppgiftssamlingar.

Innan åtkomst medges till sådana personuppgifter måste Försvarsmakten avgöra om det finns sakliga skäl att låta utländska underrättelse- och säkerhetstjänster få del av uppgifterna, dvs. om det finns behov av att lämna ut uppgifterna för att främja bekämpningen av terrorism eller andra svenska intressen. Innan uppgifterna förs över ska Försvarsmakten dessutom bedöma om det finns rättsliga förutsättningar att lämna ut uppgifterna till utländska mottagare, bl.a. om sekretess hindrar det.

Direktåtkomst enligt paragrafen får bara ske i den utsträckning det följer av lag eller förordning eller om regeringen i ett enskilt fall beslutat om det.

Direktåtkomst i andra fall

4 §

Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter eller särskilt beslut om vilka som i andra fall än de som anges i 2 § och 3 § får ha direktåtkomst till gemensamt tillgängliga uppgifter.

Paragrafen, som behandlas i avsnitt 6.5.2, är en upplysningsföreskrift om att regeringen kan meddela föreskrifter eller i ett enskilt fall besluta att direktåtkomst får medges i andra fall än de som anges i 2 och 3 §§.

Övriga bestämmelser

5 §

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela

1. ytterligare föreskrifter eller beslut i enskilda fall om omfattningen av direktåtkomsten, och

2. föreskrifter om behörighet och säkerhet vid sådan åtkomst.

Paragrafen, som behandlas i avsnitt 6.5.2, är en upplysningsföreskrift om att regeringen, eller den myndighet som regeringen bestämmer, kan meddela ytterligare föreskrifter eller beslut i enskilda fall om omfattningen av direktåtkomsten, och föreskrifter om behörighet och säkerhet vid sådan åtkomst.

4 kap. Skyldighet som personuppgiftsansvarig

Åtgärder för att säkerställa författningsenlig behandling

1 §

Försvarsmakten ska, genom lämpliga tekniska och organisatoriska åtgärder, säkerställa att behandlingen av personuppgifter är författningsenlig och skydda rättigheterna för dem som uppgifterna rör.

Paragrafen behandlas i avsnitt 6.6.1. Den reglerar, tillsammans med 2 och 3 §§, de krav som ställs på Försvarsmakten i fråga om tekniska och organisatoriska åtgärder för att säkerställa att behandlingen av personuppgifter är författningsenlig och att rättigheterna för de vars personuppgifter behandlas skyddas.

Tekniska och organisatoriska åtgärder för att skydda personuppgifterna regleras i 4 §.

Organisatoriska åtgärder som avses i paragrafen är bl.a. att anta interna strategier för dataskydd, att informera och utbilda personalen och att säkerställa en tydlig ansvarsfördelning.

Vilka åtgärder som bör vidtas får avgöras efter en bedömning i enskilda fall. Vid den bedömningen har det betydelse bl.a. vilka personuppgifter som ska behandlas, mängden uppgifter och hur integritetskänsliga de är. Även grunden för behandlingen och riskerna

med den ska beaktas. Mer långtgående åtgärder kan behövas vid behandling som kan medföra särskilda risker för integritetsintrång eller vid omfattande behandling av en stor mängd personuppgifter.

2 §

Försvarsmakten ska säkerställa att det förs loggar över personuppgiftsbehandling av gemensamt tillgängliga uppgifter. Regeringen eller den myndighet regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om loggar.

Paragrafen, som behandlas i avsnitt 6.6.2, reglerar Försvarsmaktens skyldighet att säkerställa att det för gemensamt tillgängliga uppgifter, dvs. främst i automatiserade behandlingssystem, förs loggar över vissa typer av behandlingar.

Paragrafen gäller enligt 11 § även för personuppgiftsbiträden som Försvarsmakten anlitar.

En logg är en behandlingshistorik som sparas under en viss tid. Det är en teknisk funktion i systemet som ska fungera automatiskt och som inte ska gå att ändra eller påverka på annat sätt. En logg bör vara så detaljerad att den kan användas för att utreda felaktig eller obehörig användning av personuppgifter. Syftet med loggning är dels att verka förebyggande, dels att ge den personuppgiftsansvarige möjlighet att kontrollera användningen av systemen och att upptäcka felaktig eller obehörig användning av personuppgifterna. Loggningen bör inte utformas så att den medför onödiga intrång i användarnas integritet.

Krav på loggning vid behandling av personuppgifter följer indirekt av de generella kraven på lämpliga tekniska och organisatoriska åtgärder i både 1 och 4 §§. Förevarande paragraf utgör därmed ett mer preciserat krav på loggning i vissa typer av system.

Med automatiserade behandlingssystem avses särskilt för verksamheten utformade eller anpassade behandlingssystem där personuppgifter behandlas mer eller mindre strukturerat, t.ex. verksamhetsstöd i form av dokument- och ärendehanteringssystem och olika typer av register och databaser. Standardprogram som Word, Outlook och Excel är i detta sammanhang inte att anse som automatiserade behandlingssystem och omfattas därför inte av kravet på loggning i

paragrafen. Inte heller lagringsytor som t.ex. usb-minnen och anställdas personliga mappar på den egna datorn omfattas.

Paragrafen innebär att den personuppgiftsansvarige ska säkerställa att de automatiserade behandlingssystem som används möjliggör loggning i den utsträckning som krävs och att informationen faktiskt loggas. Av 1 § följer bl.a. krav på logguppföljning. Logguppföljning ska göras systematiskt och återkommande och vara såväl förebyggande som reaktiv. Den personuppgiftsansvarige ska se till att det finns rutiner för logguppföljning.

I paragrafen finns en upplysning om att regeringen eller den myndighet regeringen bestämmer kan meddela föreskrifter om loggar.

3 §

Tillgången till personuppgifter ska alltid begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter.

Paragrafen, som behandlas i avsnitt 6.6.3, reglerar den interna tillgången till personuppgifter för dem som arbetar vid Försvarsmakten.

Paragrafen innebär att den personuppgiftsansvarige är skyldig att se till att anställda och andra som deltar i arbetet bara ges tillgång till de personuppgifter som krävs för att de ska kunna fullgöra sina arbetsuppgifter. Inom Försvarsmakten behandlas en betydande mängd personuppgifter, ofta av integritetskänsligt slag, vilka inte bör spridas till någon som inte är behörig att ta del av uppgifterna. Kravet på behörighetsbegränsning syftar till att minska den interna exponeringen av personuppgifterna. Hur det bör göras får bedömas med utgångspunkt i förutsättningarna och myndighetens behov. Faktorer som informationssystemens storlek och personuppgifternas natur ska beaktas.

Paragrafen reglerar inte bara Försvarsmaktens personals tillgång till personuppgifter. Vid direktåtkomst är det den mottagande myndigheten som ansvarar för att den egna personalen inte ges tillgång till fler personuppgifter i det informationssystem som åtkomsten avser än vad arbetsuppgifterna motiverar.

Säkerheten för personuppgifter

4 §

Försvarsmakten ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas, särskilt mot obehörig eller otillåten behandling eller förstöring och mot förlust eller annan oavsiktlig skada.

I paragrafen, som behandlas i avsnitt 6.6.4, regleras Försvarsmaktens skyldighet att genom lämpliga tekniska och organisatoriska åtgärder skydda de personuppgifter som behandlas.

Paragrafen gäller enligt 11 § även för personuppgiftsbiträden som Försvarsmakten anlitar.

Enligt paragrafen ska Försvarsmakten vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Personuppgifterna ska särskilt skyddas mot obehörig eller otillåten behandling och mot förlust, förstöring eller annan oavsiktlig skada. Uppräkningen illustrerar vad skyddsåtgärderna ska åstadkomma, men den är inte uttömmande.

Skydd mot obehörig eller otillåten behandling innebär att obehöriga personer ska vägras åtkomst till utrustning som används vid behandling, att obehörig läsning, kopiering, ändring eller radering av datamedier ska förhindras, att obehörig registrering av personuppgifter och obehörig kännedom om, ändring eller radering av lagrade personuppgifter ska förhindras och att obehörig läsning, kopiering, ändring eller radering av personuppgifter i samband med uppgiftslämnande eller transport av databärare ska förhindras. Åtgärder ska också vidtas i syfte att säkerställa att personer som är behöriga att använda ett informationssystem endast har tillgång till personuppgifter som omfattas av deras behörighet. Den personuppgiftsansvarige ska också säkerställa att det kan kontrolleras och fastställas till vilka myndigheter eller andra organ personuppgifter har överförts och för vilka myndigheter eller andra organ uppgifterna har gjorts tillgängliga och att det i efterhand kan kontrolleras och fastställas vilka personuppgifter som förts in i ett informationssystem, när det har gjorts och av vem.

Skydd mot förlust, förstöring eller annan oavsiktlig skada innebär bl.a. att de informationssystem som används ska kunna återställas

vid störningar, att systemen ska fungera och att funktionsfel rapporteras och att de lagrade personuppgifterna inte kan förvanskas genom funktionsfel i systemen.

Som exempel på organisatoriska skyddsåtgärder kan nämnas fastställandet av en säkerhetspolicy, kontroller och uppföljning av säkerheten, utbildning i datasäkerhet och information om vikten av att följa gällande säkerhetsrutiner.

Vilken skyddsnivå som är lämplig får avgöras av Försvarsmakten från fall till fall. Bedömningen är bl.a. beroende av vilka personuppgifter som behandlas och hur integritetskänsliga de är.

Dataskyddsombud

5 §

Försvarsmakten ska inom myndigheten utse ett eller flera dataskyddsombud och anmäla till tillsynsmyndigheten när dataskyddsombud utses och entledigas.

Paragrafen, som behandlas i avsnitt 6.6.5, reglerar Försvarsmaktens skyldighet att utse dataskyddsombud. Dataskyddsombud definieras i 1 kap. 8 §.

I paragrafen föreskrivs att ett eller flera dataskyddsombud ska utses. Dataskyddsombudet ska vara anställd hos Försvarsmakten.

Försvarsmakten ska anmäla till tillsynsmyndigheten när dataskyddsombud utses och entledigas.

6 §

Dataskyddsombudet ska

1. självständigt kontrollera att Försvarsmakten behandlar personuppgifter författningsenligt och på ett korrekt sätt och i övrigt fullgör sina skyldigheter,

2. informera och ge råd till Försvarsmakten och till dem som behandlar personuppgifter under myndighetens ledning om deras skyldigheter vid behandling av personuppgifter,

3. samråda med tillsynsmyndigheten, och

4. föra en förteckning över de kategorier av behandlingar som Försvarsmakten ansvarar för och som är helt eller delvis automatiserade.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om vad en förteckning som avses i första stycket 4 ska innehålla.

Om Försvarsmakten bryter mot de bestämmelser som gäller för behandlingen av personuppgifter och rättelse inte vidtas, ska dataskyddsombudet anmäla det till tillsynsmyndigheten.

I paragrafen, som behandlas i avsnitt 6.6.5, anges vilka uppgifter dataskyddsombud ska utföra.

I *punkten 1* föreskrivs att dataskyddsombud självständigt ska kontrollera att den personuppgiftsansvarige behandlar personuppgifter författningsenligt och på ett korrekt sätt och i övrigt fullgör sina skyldigheter. Det innebär att ombudet måste förvissa sig om att den personuppgiftsansvarige följer de bestämmelser som reglerar behandlingen av personuppgifter. Hur omfattande kontrollen bör vara får avgöras efter omständigheterna.

Dataskyddsombuden bör framför allt granska den faktiska hanteringen av personuppgifter. Därutöver bör ombuden exempelvis granska rutinerna för behandling av personuppgifter, hur tillgången till personuppgifter hanteras och vilka krav på utbildning och andra kvalifikationer som den personuppgiftsansvarige ställer på personal som behandlar personuppgifter. Ombudet bör påpeka eventuella brister för den personuppgiftsansvarige så att denne blir medveten om dem och har möjlighet att vidta lämpliga åtgärder.

Kravet på självständighet innebär att dataskyddsombud ska kunna utföra sina arbetsuppgifter på ett oberoende sätt. Ombudet bör framför allt ha sådan ställning i organisationen att dess synpunkter och råd tas på allvar. De förutsätts också ha goda kunskaper om regelverket om personuppgiftsbehandling.

I *punkten 2* anges att dataskyddsombudet ska informera och ge råd till den personuppgiftsansvarige och de som behandlar personuppgifter under dennes ledning om deras skyldigheter vid sådan behandling. Det handlar främst om att göra den personuppgiftsansvarige och medarbetarna medvetna om vad de i olika situationer är skyldiga att göra, t.ex. att ha säkerhetsrutiner och att dokumentera personuppgiftsbehandlingen. Det innebär inte att dataskyddsombuden

ska tala om för den personuppgiftsansvarige och medarbetarna hur de ska behandla personuppgifter i enskilda fall.

I *punkten 3* föreskrivs att dataskyddsombudet ska samråda med tillsynsmyndigheten. Det innebär att ombuden vid tveksamheter av olika slag bör fråga tillsynsmyndigheten om råd.

I *punkten 4* föreskrivs att dataskyddsombudet ska föra en förteckning över de kategorier av behandlingar som Försvarsmakten ansvarar för och som är helt eller delvis automatiserade Vad förteckningarna ska innehålla föreskrivs av regeringen eller den myndighet som regeringen bestämmer, vilket framgår av paragrafens *andra stycke*.

Av *tredje stycket* framgår att dataskyddsombudet ska anmäla till tillsynsmyndigheten om Försvarsmakten bryter mot de bestämmelser som gäller för behandlingen av personuppgifter och rättelse inte vidtas.

Personuppgiftsbiträden

7 §

Försvarsmakten får, om det är lämpligt, anlita personuppgiftsbiträden för behandling av personuppgifter på Försvarsmaktens vägnar. Innan ett personuppgiftsbiträde anlitas, ska Försvarsmakten försäkra sig om att biträdet kommer att vidta de lämpliga tekniska och organisatoriska åtgärder som krävs för att behandlingen av personuppgifter ska vara författningsenlig och för att skydda rättigheterna för den som uppgifterna rör.

Av paragrafen framgår att personuppgiftsbiträden får anlitas om det är lämpligt och vad Försvarsmakten måste göra innan ett personuppgiftsbiträde anlitas. Personuppgiftsbiträde definieras i 1 kap. 8 §. Paragrafen behandlas i avsnitt 6.6.6.

Försvarsmakten får anlita personuppgiftsbiträden under förutsättning att det är lämpligt. Om det är lämpligt får avgöras med hänsyn bl.a. till vilka personuppgifter som ska behandlas. Paragrafen föreskriver att Försvarsmakten ska försäkra sig om att biträdet vidtar lämpliga tekniska och organisatoriska åtgärder för att personuppgiftsbehandlingen ska vara författningsenlig och för att skydda registrerades rättigheter. Kraven omfattar inte bara säkerhetsåtgärder, utan även andra tekniska och organisatoriska åtgärder. Skyldigheten

innebär att den personuppgiftsansvarige, innan ett personuppgiftsbiträde anlitas, bl.a. bör förhöra sig om hur biträdet kommer att behandla uppgifterna tekniskt, hur arbetet är organiserat och vilket skydd personuppgifterna kommer att ha.

Som framgår av 11 § gäller skyldigheten att logga behandling av personuppgifter enligt 2 § även för personuppgiftsbiträden som Försvarsmakten anlitar.

8 §

Personuppgiftsbiträdets behandling av personuppgifter ska regleras i ett skriftligt avtal eller annan skriftlig överenskommelse.

Paragrafen reglerar förhållandet mellan Försvarsmakten och personuppgiftsbiträden. Den behandlas i avsnitt 6.6.6.

Det ska finnas ett skriftligt avtal eller en annan skriftlig överenskommelse med personuppgiftsbiträden som reglerar personuppgiftsbiträdets behandling av personuppgifter för Försvarsmaktens räkning. Eftersom statliga myndigheter, som är enheter inom samma juridiska person, i rättslig mening inte kan ingå bindande avtal med varandra får de träffa en skriftlig överenskommelse som reglerar behandlingen om en myndighet agerar personuppgiftsbiträde åt en annan.

9 §

Ett personuppgiftsbiträde får inte anlita ett annat personuppgiftsbiträde utan skriftligt tillstånd av Försvarsmakten.

Av paragrafen, som behandlas i avsnitt 6.6.6, föreskrivs att personuppgiftsbiträdet inte utan skriftligt tillstånd från Försvarsmakten får anlita ett annat personuppgiftsbiträde, ett s.k. underbiträde. Ett sådant tillstånd kan gälla biträdets rätt att anlita underbiträden generellt eller i en specifik situation. Syftet med bestämmelsen är att Försvarsmakten ska känna till vilka personuppgiftsbiträden som behandlar personuppgifter för dennes räkning.

10 §

Ett personuppgiftsbiträde eller den eller de personer som arbetar under biträdets eller Försvarsmaktens ledning ska behandla personuppgifter i enlighet med instruktioner från Försvarsmakten.

Om ett personuppgiftsbiträde, i strid med Försvarsmaktens instruktioner, bestämmer ändamålen med och medlen för behandlingen, ska biträdet anses vara personuppgiftsansvarig enligt denna lag för den behandlingen.

Paragrafen, som behandlas i avsnitt 6.6.6, reglerar vad som gäller vid behandling av personuppgifter hos ett personuppgiftsbiträde.

Av *första stycket* framgår den grundläggande principen att ett personuppgiftsbiträde och den eller de personer som arbetar under biträdets ledning bara får behandla personuppgifter i enlighet med instruktioner från den personuppgiftsansvarige. Instruktionerna till biträdet bör vara så tydliga att det inte finns risk för otillåten behandling. Instruktionerna kan exempelvis gälla hur tillgången till personuppgifter hos biträdets anställda ska begränsas, om biträdet ska använda kryptering vid kommunikation och andra åtgärder som krävs för dataskydd. Om det finns avvikande regler i annan lagstiftning som föreskriver att personuppgiftsbiträdet är skyldig att utföra viss behandling, t.ex. att lämna ut allmänna handlingar, får behandlingen utföras utan särskilda instruktioner.

I *andra stycket* regleras det fallet där personuppgiftsbiträdet i strid med den personuppgiftsansvariges instruktioner bestämmer ändamålen med och medlen för behandlingen. Personuppgiftsbiträdet är då att anse som personuppgiftsansvarig för den behandlingen.

11 §

Det som sägs om Försvarsmaktens skyldigheter i 2–4 §§ gäller även för personuppgiftsbiträden som Försvarsmakten anlitar.

Paragrafen kopplar Försvarsmaktens skyldigheter i egenskap av personuppgiftsansvarig till att gälla även för personuppgiftsbiträden. Vad som närmare gäller för personuppgiftsbiträdet framgår således av kommentarerna till 2–4 §§.

Att personuppgiftsbiträden åläggs vissa skyldigheter fråntar inte Försvarsmakten dess ansvar. Försvarsmakten är, som framgår av kommentaren till 1 kap. 6 §, ansvarig för den behandling av personuppgifter som personuppgiftsbiträdet utför på myndighetens vägnar.

Den omständigheten att personuppgiftsbiträden ges en direkt skyldighet att vidta vissa åtgärder innebär dock att tillsynsmyndigheten vid brister kan vidta åtgärder mot både personuppgiftsbiträdet och Försvarsmakten.

5 kap. Enskildas rättigheter

Rätten till information

Allmän information

1 §

Försvarsmakten ska göra följande allmänna information tillgänglig.

1. Myndighetens identitet och kontaktuppgifter.

2. Uppgifter om dataskyddsombudet.

3. Ändamålen med behandlingen.

4. Rätten enligt 3 § att begära att få information om behandling av personuppgifter och att få del av dem.

5. Rätten att begära rättelse, radering eller begränsning av behandlingen enligt 6 §.

I paragrafen, som behandlas i avsnitt 6.7.1, anges vilken allmän information som Försvarsmakten på eget initiativ ska göra tillgänglig. Informationen, som riktar sig till allmänheten, kan göras tillgänglig t.ex. på myndighetens webbplats.

Enligt *punkten 1* ska myndighetens identitet och kontaktuppgifter göras tillgängliga. Med det avses uppgifter om myndighetens namn, postadress, telefonnummer och e-postadress.

Försvarsmakten är enligt 4 kap. 5 § skyldig att utse dataskyddsombud. Enligt *punkten 2* ska uppgifter om dataskyddsombudet anges. Det behöver inte vara en kontaktuppgift direkt till dataskyddsombudet, t.ex. hans eller hennes e-postadress, utan det är tillräckligt att ombudet går att nå med hjälp av uppgifterna.

I *punkten 3* föreskrivs att ändamålen med behandlingen ska framgå. Det är inte ändamålen med behandlingen av personuppgifter i enskilda

fall som avses utan för vilka typer av ändamål som myndigheten behandlar personuppgifter. Det kan vara underrättelsearbete och åtgärder inom ett särskilt verksamhetsområde eller åtgärder som vidtas inom ramen för säkerhetsskyddsarbetet, exempelvis säkerhetsprövning och registerkontroll.

I *punkterna 4 och 5* föreskrivs att Försvarsmakten ska upplysa om de rättigheter som enskilda har enligt 3 och 6 §§. Det gäller rätten att få information om behandlingen av personuppgifter och att få del av dem samt rätten att begära rättelse, radering eller begränsning av behandlingen.

Information som ska lämnas om uppgifterna samlas in från personen själv

2 §

Om uppgifter om en person samlas in från personen själv, ska Försvarsmakten när personuppgifterna erhålls, självmant lämna följande information till den som uppgifterna rör:

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 som uppgifterna rör ska 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.

Paragrafen behandlas i avsnitt 6.7.2.

Den information som Försvarsmakten självmant ska lämna en enskild då personuppgifter samlats in från den enskilde själv ska omfatta uppgifter om att det är Försvarsmakten som är ansvarig för personuppgiftsbehandlingen, ändamålen med behandlingen samt övrig information som behövs för att den registrerade ska kunna ta till vara sina rättigheter. Denna informationsskyldighet förutsätter att personuppgifter samlas in från den som uppgifterna rör vid någon form av direktkontakt med denne.

Information som ska lämnas efter begäran

3 §

Försvarsmakten är skyldig att en gång per kalenderår till den som begär det lämna skriftligt besked om personuppgifter som rör honom eller henne behandlas. Behandlas sådana uppgifter ska sökanden få del av dem och få följande skriftliga information.

1. Vilka personuppgifter om den sökande som behandlas.

2. Varifrån personuppgifterna kommer.

3. Den rättsliga grunden för behandlingen.

4. Ändamålen med behandlingen.

5. Mottagare eller kategorier av mottagare av personuppgifterna, även i annat land eller internationella organisationer.

6. Hur länge personuppgifterna får behandlas eller, om det inte är möjligt att ange, kriterierna för att fastställa det.

7. Rätten att begära rättelse, radering eller begränsning av behandlingen enligt 6 §.

Utlämnande enligt första stycket behöver inte omfatta personuppgifter som sökanden har tagit del av, om inte han eller hon begär det. Det ska dock framgå av informationen att personuppgifterna i fråga behandlas.

En ansökan enligt första stycket ska göras skriftligen hos Försvarsmakten och vara undertecknad av den sökande själv. Information enligt första stycket ska 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.

I paragrafen regleras enskildas rätt att en gång per kalenderår få besked om huruvida deras personuppgifter behandlas, att få del av sådana uppgifter och att få viss information om behandlingen av dem.

Paragrafen behandlas i avsnitt 6.7.2.

I *första stycket* anges vilken information sökanden kan få del av.

I *andra stycket* undantas sådana personuppgifter som sökanden har tagit del av från skyldigheten att lämna ut uppgifterna. Sökanden ska dock informeras om att personuppgifterna i fråga behandlas.

I 7 § föreskrivs att informationen ska lämnas till den uppgifterna rör avgiftsfritt en gång per år och att begäran därutöver kan avslås.

Beslut att vägra att lämna information får enligt 7 kap. 2 § överklagas.

Av *tredje stycket* framgår kraven på en begäran om information.

Begränsning av rätten till information

4 §

Informationsskyldigheten i 2 och 3 §§ gäller inte i den utsträckning sekretess hindrar att uppgifterna lämnas ut.

Om förutsättningarna i första stycket är uppfyllda, är Försvarsmakten inte skyldig att lämna ut skälen för beslut enligt första stycket eller beslut i fråga om rättelse, radering eller begränsning av behandlingen enligt 6 §.

I paragrafen, som behandlas i avsnitt 6.7.4, görs undantag från Försvarsmaktens informationsskyldighet på grund av sekretess.

Många uppgifter som behandlas i Försvarsmaktens olika verksamheter omfattas av utrikessekretess och försvarssekretess enligt 15 kap. 1 och 2 §§ offentlighets- och sekretesslagen (2009:400). Informationsskyldigheten gäller enligt *första* stycket inte i den utsträckning sekretess hindrar att uppgifterna lämnas ut till den som uppgifterna rör.

Enligt *andra stycket* är Försvarsmakten inte heller skyldig att lämna ut skälen för beslut enligt första stycket och beslut i fråga om rättelse, radering eller begränsning av behandlingen om motiveringen skulle riskera att skada något av de intressen som sekretessen avser att skydda.

5 §

Informationsskyldigheten i 2 och 3 §§ gäller inte personuppgifter i löpande text som inte fått sin slutliga utformning när begäran gjordes eller som utgör minnesanteckning eller liknande.

Informationsskyldigheten gäller dock om uppgifterna har lämnats ut till tredje part, behandlas enbart för vetenskapliga, statistiska eller historiska ändamål eller arkivändamål av allmänt intresse eller, när det gäller löpande text som inte fått sin slutliga utformning, om uppgifterna har behandlats längre än ett år.

I paragrafen, som behandlas i avsnitt 6.7.4, föreskrivs i första stycket undantag från informationsskyldigheten i 2 och 3 §§ för personuppgifter i viss typ av text. Undantaget gäller dock enligt andra stycket inte i vissa fall.

Den personuppgiftsansvariges skyldighet att lämna personrelaterad information enligt 2 och 3 §§ gäller enligt *första stycket* inte för personuppgifter i löpande text som inte fått sin slutliga utformning när begäran gjordes eller text som utgör minnesanteckningar eller liknande. Med löpande text avses information som inte har strukturerats så att sökning av personuppgifter underlättas. Bild- och ljudupptagningar omfattas inte av undantaget eftersom det bara gäller text. Med text som inte fått sin slutliga utformning avses koncept eller utkast till protokoll, skrivelser, beslut eller liknande. Löpande text som är avsedd att tidvis ändras eller kompletteras och därför aldrig får någon slutlig utformning omfattas inte. Det sistnämnda kan t.ex. vara diarier, journaler, register eller förteckningar som förs löpande. Med minnesanteckning avses anteckningar som utgör hjälpmedel för handläggningen, t.ex. promemorior och andra anteckningar eller upptagningar som har skapats bara för att förbereda ett ärende för avgörande och som inte har tillfört ärendet något i sak.

Av *andra stycket* framgår att undantaget från informationsskyldigheten inte gäller under vissa förhållanden. Sökanden har då rätt att få del av personuppgifter även i ofärdig löpande text eller som utgör minnesanteckningar och liknande. Undantaget gäller inte om personuppgifterna har lämnats ut till tredje part. Tredje part definieras i 1 kap. 8 §. Det är den version av uppgifterna i t.ex. utkastet som lämnades till tredje part som informationsskyldigheten omfattar, även om utkastet därefter har ändrats.

Vidare gäller inte undantaget om personuppgifterna behandlas enbart för vetenskapliga, statistiska eller historiska ändamål eller arkivändamål av allmänt intresse. Om ett ärende har avslutats och utkastet eller minnesanteckningen har arkiverats eller om handlingarna endast används vid statistikproduktion eller forskning ska alltså information om behandlingen av personuppgifterna lämnas ut. Undantaget gäller inte heller för löpande text som inte fått sin slutliga utformning, om personuppgifterna har behandlats under längre tid än ett år.

Det är tidpunkten för begäran som är avgörande för bedömningen av om något av undantagen gäller. Både ettårsfristen och frågan om uppgifterna har lämnats ut till tredje part eller behandlas för vetenskapliga, statistiska eller historiska ändamål eller arkivändamål av allmänt intresse ska bedömas i förhållande till när begäran om information gjordes.

Rätten till rättelse, radering och begränsning av behandlingen

6 §

Försvarsmakten ska på begäran av den som personuppgiften rör snarast rätta, radera eller begränsa sådana personuppgifter som inte har behandlats i enlighet med denna lag eller föreskrifter som har meddelats med stöd av lagen.

Försvarsmakten ska också underrätta tredje part till vilken uppgifterna har lämnats ut om åtgärden, om den som personuppgiften rör begär det eller om en mera betydande skada eller olägenhet för denne skulle kunna undvikas genom en underrättelse.

Någon underrättelse behöver dock inte lämnas, om sekretess hindrar det eller detta är omöjligt eller skulle innebära en oproportionerligt stor arbetsinsats.

Paragrafen reglerar enskildas rätt att begära rättelse, radering eller begränsning av personuppgifter som inte har behandlats i enlighet med denna lag. Paragrafen behandlas i avsnitt 6.7.5.

Försvarsmakten ska enligt *första stycket* på begäran av den som personuppgiften rör snarast rätta, radera eller begränsa sådana personuppgifter som inte har behandlats i enlighet med denna lag eller föreskrifter som har meddelats med stöd av lagen. Begäran kan framställas formlöst.

Den personuppgiftsansvarige är såsom framgår av paragrafens *andra stycke* skyldig att underrätta tredje part om en korrigering, om den uppgiften rör begär det eller det kan antas att en underrättelse skulle kunna undvika mera betydande skada eller olägenhet för den registrerade. Gäller det däremot en mera harmlös uppgift bör det som regel krävas någon särskild omständighet för att man ska kunna anta att en underrättelse skulle kunna undvika sådan skada eller

olägenhet som avses. Det måste vidare kunna antas att underrättelsen medför att skadan eller olägenheten kan undvikas. Detta är inte fallet när det är känt att aktuella tredje män redan har korrigerat uppgiften.

Enligt *tredje stycket* behöver inte någon underrättelse lämnas, om sekretess hindrar det eller detta är omöjligt eller skulle innebära en oproportionerligt stor arbetsinsats. Vad som gäller vid sekretess framgår av 4 §. Vad som är att betrakta som en oproportionerligt stor arbetsinsats får bedömas från fall till fall och vid eventuell granskning eller överprövning.

Beslut i fråga om rättelse eller radering av personuppgifter eller begränsning av behandlingen får enligt 7 kap. 2 § överklagas.

Avgiftsfri information

7 §

Information enligt 1 och 2 §§ ska lämnas utan avgift.

Information och uppgifter enligt 3 § ska lämnas utan avgift en gång per kalenderår. Om någon begär information och uppgifter enligt 3 § oftare än en gång per kalenderår, får Försvarsmakten avslå begäran.

Paragrafen behandlas i avsnitt 6.7.6.

Enligt *första stycket* ska information enligt 1 och 2 §§ lämnas utan att myndigheten har rätt att ta ut någon avgift.

Försvarsmakten är även enligt 3 § skyldig att till var och som ansöker om det, en gång per kalenderår gratis lämna besked om huruvida personuppgifter som rör den sökande behandlas eller inte.

Enligt *andra stycket* i förevarande paragraf anges att rätten gäller en begäran per kalenderår och att Försvarsmakten har rätt att avslå ytterligare begäran inom samma kalenderår. Försvarsmaktens prövning i en sådan situation begränsas till att kontrollera huruvida personen har begärt uppgifter tidigare under året och att i sådant fall meddela ett avslagsbeslut.

6 kap. Tillsyn

Tillsyn över personuppgiftsbehandlingen

1 §

Den myndighet som regeringen bestämmer ska utöva allmän tillsyn över Försvarsmaktens behandling av personuppgifter enligt denna lag.

Tillsynsmyndigheten ska ge råd och stöd till Försvarsmakten om myndighetens skyldigheter enligt lag eller annan författning eller när det i övrigt är påkallat.

I paragrafen, som behandlas i avsnitt 6.8.1, anges vilka tillsynsuppgifter som tillsynsmyndigheten har.

Enligt *första stycket* ska tillsynsmyndigheten utöva allmän tillsyn över Försvarsmaktens behandling av personuppgifter enligt denna lag. Tillsynsmyndigheten avgör om och i vilken utsträckning tillsyn ska utövas och hur den ska genomföras. Myndigheten ska agera helt oberoende vid denna bedömning. Det innebär att ingen kan kräva att myndigheten ska utöva tillsyn. Det finns inte heller några formella krav på hur tillsynen ska utövas, med undantag från vissa bestämmelser i denna lag och i föreskrifter som beslutas i anslutning till den.

Enligt *andra stycket* ska tillsynsmyndigheten ge råd och stöd till Försvarsmakten. Med råd avses både muntliga och skriftliga råd. Det kan vara fråga om allmänna råd eller rådgivning i ett enskilt fall. Myndigheten ska ge råd och stöd bara när den anser att det är påkallat. Rådgivningen och stödet ska avse personuppgiftsansvarigas och personuppgiftsbiträdens skyldigheter. Paragrafen ger således ingen rätt för personuppgiftsansvariga eller personuppgiftsbiträden att avkräva tillsynsmyndigheten råd i en konkret fråga.

Befogenheter

Utredningsbefogenheter

2 §

Tillsynsmyndigheten har rätt att av Försvarsmakten eller ett personuppgiftsbiträde på begäran få

1. tillgång till personuppgifter som behandlas,

2. upplysningar om och dokumentation av behandlingen av personuppgifter och säkerhets- och skyddsåtgärder,

3. tillträde till sådana lokaler som har anknytning till behandling av personuppgifter och tillgång till utrustning och andra medel för behandling av personuppgifter, och

4. det biträde och annan information som behövs för tillsynen.

I paragrafen, som behandlas i avsnitt 6.8.1, regleras tillsynsmyndighetens undersökningsbefogenheter.

Enligt *punkten 1* har tillsynsmyndigheten rätt att för sin tillsyn från personuppgiftsansvariga och personuppgiftsbiträden få tillgång till alla personuppgifter som behandlas. Det innebär att Försvarsmakten eller personuppgiftsbiträdet ska lämna de begärda uppgifterna även om det kräver viss efterforskning. Att tillsynsmyndigheten har rätt få del av annan information framgår av punkterna 2 och 4 och rätten att få hjälp med de sökningar i behandlingssystem som myndigheten begär regleras i punkten 4.

Punkten 2 ger tillsynsmyndigheten rätt till upplysningar och dokumentation som rör behandling av personuppgifter och vilka åtgärder som har vidtagits för att säkerställa skyddet för personuppgifterna och registrerades personliga integritet. Dokumentationen kan avse exempelvis de register eller loggar som Försvarsmakten och personuppgiftsbiträden ska föra. Det kan också vara fråga om upplysningar om och dokumentation av vilka organisatoriska och tekniska åtgärder som vidtogs i samband med att en viss typ av behandling påbörjades. Det kan också röra sig om åtgärder för att garantera säkerheten, begränsa den interna tillgången till uppgifter eller förhindra otillåten behandling och åtgärder för intern kontroll. Informationen kan avse exempelvis ändamålen med behandlingen eller loggar och förteckningar över pågående behandlingar

I *punkten 3* regleras tillsynsmyndighetens rätt att få tillträde till lokaler som den personuppgiftsansvarige eller personuppgiftsbiträdet disponerar och tillgång till utrustning och andra medel som används för behandlingen. Rätten till tillträde ger inte myndigheten rätt att bereda sig tillträde med tvång. Om Försvarsmakten eller personuppgiftsbiträdet inte samarbetar kan tillsynsmyndigheten utnyttja sina korrigerande befogenheter enligt 4 §. Tillsynsmyndigheten har också rätt att få tillgång till den utrustning som tillsynsobjektet disponerar

för att, med hjälp av tillsynsobjektets personal, kunna göra nödvändiga körningar och kontroller. Punkten ger således inte tillsynsmyndigheten någon rätt att fritt använda tillsynsobjektets utrustning och datasystem.

Punkten 4 klargör att tillsynsmyndigheten har rätt att få hjälp med de sökningar och andra åtgärder som den begär och annan nödvändig hjälp för att genomföra tillsynen. Paragrafen ger även tillsynsmyndigheten rätt till information som inte har direkt anknytning till behandlingen av personuppgifter men som myndigheten behöver för tillsynen. Informationen kan avse t.ex. verksamhetsplaner som beskriver den verksamhet där behandlingen utförs.

Förebyggande befogenheter

3 §

Om tillsynsmyndigheten bedömer att det finns risk för att personuppgifter kan komma att behandlas i strid med lag eller annan författning, ska myndigheten genom råd, rekommendationer eller påpekanden försöka förmå Försvarsmakten eller personuppgiftsbiträdet att vidta åtgärder för att minska den risken.

Tillsynsmyndigheten får utfärda en skriftlig varning för att planerad behandling av personuppgifter riskerar att stå i strid med lag eller annan författning. Detsamma gäller om pågående behandling riskerar att stå i strid med lag eller annan författning.

Paragrafen reglerar tillsynsmyndighetens befogenheter i det förebyggande arbetet. De åtgärder som regleras i paragrafen är inte av tvingande karaktär. De syftar till att förebygga att framtida behandling av personuppgifter står i strid med de bestämmelser som gäller för behandlingen. Paragrafen behandlas i avsnitt 6.8.1.

Av *första stycket* framgår att tillsynsmyndigheten, om det finns risk för att personuppgifter kan komma att behandlas i strid med lag eller annan författning, ska försöka förmå Försvarsmakten eller personuppgiftsbiträdet att minska risken genom råd, rekommendationer och påpekanden. Rådgivning kan avse såväl formella som informella samråd.

Av 4 § första stycket 1 framgår att de befogenheter som räknas upp i detta stycke även i vissa fall får användas i korrigerande syfte.

Enligt *andra stycket* får tillsynsmyndigheten skriftligen varna för att viss behandling riskerar att strida mot meddelade föreskrifter. En varning är en mer ingripande åtgärd än åtgärderna i första stycket. Varning kan användas för att visa hur allvarligt tillsynsmyndigheten ser på den planerade behandlingen. Tillsynsmyndigheten behöver inte ha uttömt andra förebyggande åtgärder innan den utfärdar en varning. En varning ska vara skriftlig. Av den ska framgå varför tillsynsmyndigheten bedömt att behandlingen inte kommer att vara författningsenlig. Åtgärden är inte tvingande, men den som får en varning förväntas rätta sig efter den.

Korrigerande befogenheter

4 §

Om tillsynsmyndigheten konstaterar att personuppgifter behandlas i strid med lag eller annan författning, eller att Försvarsmakten eller ett personuppgiftsbiträde annars inte fullgör sina skyldigheter, får tillsynsmyndigheten

1. genom sådana åtgärder som anges i 3 § första stycket försöka förmå Försvarsmakten eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsenlig eller att uppfylla andra skyldigheter, eller

2. förelägga Försvarsmakten eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsenlig eller att fullgöra andra skyldigheter.

Om ett föreläggande utfärdas ska det av föreläggandet framgå när åtgärderna senast ska vara genomföras och, om det är lämpligt, vilka åtgärder som ska vidtas.

I paragrafen regleras tillsynsmyndighetens korrigerande befogenheter. Paragrafen, behandlas i avsnitt 6.8.1.

Tillsynsmyndigheten har möjlighet att successivt använda olika medel och därigenom stegra påtryckningarna på den som inte självmant rättar sig.

De korrigerande befogenheterna får användas om tillsynsmyndigheten konstaterar att Försvarsmakten eller ett personuppgiftsbiträde behandlar personuppgifter i strid med lag eller annan författning eller annars inte fullgör sina skyldigheter. De skyldigheter som

avses är framför allt skyldigheterna i 4 kap. Försvarsmakten har emellertid också skyldigheter enligt 2 och 5 kap. och skyldighet att bistå tillsynsmyndigheten enligt 2 §. Även underlåtenhet att fullgöra sådana skyldigheter med anledning av denna lag omfattas.

Enligt *första stycket punkten 1* får tillsynsmyndigheten använda de förebyggande befogenheter som regleras i 3 § första stycket för att försöka förmå den Försvarsmakten eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsenlig eller att uppfylla andra skyldigheter.

Enligt *punkten 2* får tillsynsmyndigheten förelägga Försvarsmakten eller personuppgiftsbiträdet att vidta åtgärder för att viss behandling av personuppgifter ska bli författningsenlig eller för att de ska uppfylla andra skyldigheter.

I *andra stycket* föreskrivs att det av ett föreläggande alltid ska framgå när åtgärderna senast ska vara genomförda och, om det är lämpligt, vilka åtgärder som ska vidtas. Om föreläggandet avser rättelse, radering eller begränsning av behandlingen bör det framgå av föreläggandet vad som ska göras. Tillsynsmyndigheten får emellertid överlåta åt Försvarsmakten eller personuppgiftsbiträdet att avgöra vilka åtgärder som ska vidtas för att behandlingen ska bli författningsenlig eller hur andra skyldigheter ska fullgöras.

7 kap. Skadestånd och överklagande

Skadestånd

1 §

Den personuppgiftsansvarige ska ersätta den som personuppgiften rör för skada och kränkning av den personliga integriteten som orsakats av behandling av personuppgifter i strid med denna lag, eller föreskrifter som har meddelats i anslutning till den.

Ersättningsskyldigheten kan i den utsträckning det är skäligt, jämkas om den personuppgiftsansvarige visar att felet inte berodde på denne.

I paragrafen regleras den registrerades rätt till skadestånd för behandling av personuppgifter i strid med regelverket. Paragrafen behandlas i avsnitt 6.9.1.

Rätt till skadestånd kan uppkomma på grund av behandling i strid med bestämmelser i denna lag eller föreskrifter som meddelats i anslutning till lagen. För att den personuppgiftsansvarige ska bli ersättningsskyldig måste den som personuppgifterna rör bevisa att behandling av dennes personuppgifter stått i strid med reglerna om personuppgiftsbehandling och att den har skadat eller kränkt honom eller henne.

Den registrerades rätt till skadestånd omfattar ersättning för kränkning av den personliga integriteten och för annan skada. Med skada avses personskada, sakskada eller ren förmögenhetsskada.

Det är bara sådan kränkning eller skada som behandlingen av personuppgifter har vållat som ersätts.

Ersättningen för kränkning får uppskattas efter skälighet mot bakgrund av samtliga omständigheter i det enskilda fallet. Sådana faktorer som att det funnits risk för otillbörlig spridning av känsliga eller felaktiga personuppgifter eller att den som uppgifterna rör genom behandlingen av uppgifterna drabbats av beslut eller åtgärder som kunnat få negativa följder hör till det som bör beaktas.

Överklagande

2 §

Försvarsmaktens beslut om information som ska lämnas enligt 5 kap. 2 och 3 §§ och om rättelse och underrättelse till tredje part enligt 5 kap. 6 § får överklagas hos allmän förvaltningsdomstol. Andra beslut enligt denna lag får inte överklagas.

Prövningstillstånd krävs vid överklagande till kammarrätten.

I paragrafen, som behandlas i avsnitt 6.9.2, anges i vilken utsträckning beslut som Försvarsmakten har fattat i egenskap av personuppgiftsansvarig får överklagas.

Vilka typer av beslut som får överklagas räknas upp i *första stycket*. Uppräkningen är uttömmande.

Besluten ska överklagas till allmän förvaltningsdomstol. Vilken förvaltningsdomstol som är behörig framgår av 14 § förordningen (1977:937) om allmänna förvaltningsdomstolars behörighet m.m. För prövning i kammarrätten krävs det enligt *andra stycket* prövningstillstånd.

3 §

Av 6 kap. 8 § offentlighets- och sekretesslagen (2009:400) följer att beslut om sekretess överklagas till kammarrätt.

Paragrafen upplyser om att beslut i frågor om sekretess överklagas direkt till kammarrätt som första överprövningsinstans.

8.2 Förslaget till lag om behandling av personuppgifter vid Försvarets radioanstalt

1 kap. Allmänna bestämmelser

Syftet med lagen

1 §

Syftet med denna lag är att säkerställa att Försvarets radioanstalt kan behandla personuppgifter på ett ändamålsenligt sätt och att skydda fysiska personers grundläggande fri- och rättigheter i samband med sådan behandling.

Bestämmelsen motsvarar 1 kap. 1 § i förslaget till lag om behandling av personuppgifter vid Försvarsmakten. För en kommentar hänvisas till den bestämmelsen.

Lagens tillämpningsområde

2 §

Denna lag gäller vid behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet samt informationssäkerhetsverksamhet.

Paragrafen reglerar, tillsammans med 3 §, lagens tillämpningsområde. Den behandlas i avsnitt 6.2.3.

I paragrafen anges att lagen gäller vid Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet samt informationssäkerhetsverksamhet.

Vad som är en personuppgift och behandling av personuppgifter definieras i 8 §.

Omfattningen av Försvarets radioanstalts uppgifter, som framgår av 1–4 §§ förordningen (2007:937) med instruktion för Försvarets radioanstalt, utvecklas närmare i avsnitt 3.2 och 6.2.3.

3 §

Lagen gäller vid sådan behandling av personuppgifter som 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.

Bestämmelsen motsvarar 1 kap. 3 § i förslaget till lag om behandling av personuppgifter vid Försvarsmakten. För en kommentar hänvisas till den bestämmelsen.

4 §

Vid behandling av personuppgifter enligt denna lag gäller inte lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

Paragrafen behandlas i avsnitt 6.2.4. Den upplyser om att lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning inte gäller när personuppgifter behandlas enligt lagen om behandling av personuppgifter vid Försvarets radioanstalt.

Förhållandet till annan reglering

5 §

Bestämmelserna i denna lag ska inte tillämpas i den utsträckning det skulle inskränka skyldigheten enligt 2 kap. tryckfrihetsförordningen att lämna ut personuppgifter.

Bestämmelsen motsvarar 1 kap. 5 § i förslaget till lag om behandling av personuppgifter vid Försvarsmakten. För en kommentar hänvisas till den bestämmelsen.

Personuppgiftsansvar

6 §

Försvarets radioanstalt är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför.

Personuppgiftsansvaret omfattar all behandling av personuppgifter som utförs under myndighetens ledning eller på dess vägnar.

Bestämmelsen motsvarar 1 kap. 6 § i förslaget till lag om behandling av personuppgifter vid Försvarsmakten. För en kommentar hänvisas till den bestämmelsen.

7 §

Försvarets radioanstalt får vara gemensamt personuppgiftsansvarig med annan endast i den utsträckning det följer av lag eller förordning eller om regeringen i ett enskilt fall beslutar om det.

Bestämmelsen motsvarar 1 kap. 7 § i förslaget till lag om behandling av personuppgifter vid Försvarsmakten. För en kommentar hänvisas till den bestämmelsen.

Definitioner

8 §

I paragrafen, som behandlas i avsnitt 6.2.9, definieras vissa uttryck som används i lagen.

Bestämmelsen motsvarar 1 kap. 8 § i förslaget till lag om behandling av personuppgifter vid Försvarsmakten. För en kommentar hänvisas till den bestämmelsen.

2 kap. Behandling av personuppgifter

Rättsliga grunder

Försvarsunderrättelseverksamhet

1 §

Personuppgifter får behandlas i Försvarets radioanstalts försvarsunderrättelseverksamhet om det är nödvändigt för att bedriva den verksamhet som anges i lagen (2000:130) om försvarsunderrättelseverksamhet och lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet.

Paragrafen behandlas i avsnitt 6.3.6.

Paragrafen anger de ändamål för vilka personuppgifter får användas i försvarsunderrättelseverksamheten genom en hänvisning till lagen (2000:130) om försvarsunderrättelseverksamhet och lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet.

Enligt 1 § lagen om försvarsunderrättelseverksamhet ska försvarsunderrättelseverksamhet bedrivas till stöd för svensk utrikes-, säkerhets- och försvarspolitik samt i övrigt för kartläggning av yttre hot mot landet. Det anges vidare att i verksamheten ingår att medverka i svenskt deltagande i internationellt säkerhetssamarbete och att försvarsunderrättelseverksamheten endast får avse utländska förhållanden.

Försvarets radioanstalt ska enligt 2 § förordningen (2008:923) om signalspaning i försvarsunderrättelsetjänst bedriva den verksamhet som avses i 1 § lagen om signalspaning i försvarsunderrättelseverksamhet. Enligt andra stycket i den paragrafen får signalspaning i försvarsunderrättelseverksamhet ske endast i syfte att kartlägga

1. yttre militära hot mot landet,
2. förutsättningar för svenskt deltagande i fredsfrämjande och humanitära insatser eller hot mot säkerheten för svenska intressen vid genomförandet av sådana insatser,
3. strategiska förhållanden avseende internationell terrorism och annan grov gränsöverskridande brottslighet som kan hota väsentliga nationella intressen,
4. utveckling och spridning av massförstörelsevapen, krigsmateriel och produkter som avses i lagen (2000:1064) om kontroll av produkter med dubbla användningsområden och av tekniskt bistånd,
5. allvarliga yttre hot mot samhällets infrastruktur,

6. konflikter utomlands med konsekvenser för internationell säkerhet,

7. främmande underrättelseverksamhet mot svenska intressen, eller

8. främmande makts agerande eller avsikter av väsentlig betydelse för svensk utrikes-, säkerhets- och försvarspolitik.

Regeringen bestämmer försvarsunderrättelseverksamhetens inriktning.

Försvarsunderrättelseverksamheten ska 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.

I underrättelseverksamhetens natur ligger att det inte går att på förhand göra tydliga avgränsningar av vilka uppgifter som måste inhämtas för att nå det slutliga målet att åstadkomma de underrättelser som uppdragsgivarna efterfrågar. Inhämtad information kan motivera inhämtning av annan information som man från början inte kände till. Det kan också uppkomma behov av att värdera trovärdigheten hos källor, som man heller inte kände till från början. Verksamheten kan också gå ut på att leta efter företeelser och hot som är okända men som antas existera.

2 §

De personuppgifter som Försvarets radioanstalt har fått tillgång till i myndighetens försvarsunderrättelseverksamhet får fortsatt behandlas i den verksamheten, om det behövs för att fullgöra den.

Vad som sägs i första stycket gäller endast om inget annat följer av denna lag eller förordning som regeringen har meddelat i anslutning till lagen.

Paragrafen behandlas i avsnitt 6.3.6.

Av paragrafens *första stycke* framgår att de personuppgifter som Försvarets radioanstalt har fått tillgång till i myndighetens försvarsunderrättelseverksamhet som huvudregel får fortsatt behandlas i den verksamheten om det behövs för att fullgöra den. Detta möjliggör för Försvarets radioanstalt att i sin försvarsunderrättelseverksamhet behandla äldre information, inklusive personuppgifter, för att förstå

och bedöma den underrättelsemässiga relevansen av den information som inhämtas.

En förutsättning för behandlingen enligt bestämmelsen är att den inte strider mot någon annan bestämmelse i lagen eller tillhörande förordning. Detta tydliggörs i *andra stycket*.

3 §

Personuppgifter som behandlas med stöd av 1 och 2 §§ får även behandlas om det är nödvändigt för att tillhandahålla information som behövs

1. i verksamhet hos berörda myndigheter som avses i 2 § första stycket lagen (2000:130) om försvarsunderrättelseverksamhet,

2. med anledning av samarbete med andra länder och internationella organisationer enligt lagen (2000:130) om försvarsunderrättelseverksamhet och lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet,

3. i utvecklingsverksamheten för de ändamål som anges i 4 §,

4. i informationssäkerhetsverksamheten för de ändamål som anges i 6 §, eller

5. för att biträda andra myndigheter i den utsträckning det följer av lag eller förordning eller om regeringen i ett enskilt fall beslutar om det.

Paragrafen behandlas i avsnitt 6.3.6.

Paragrafen ger uttryckligt rättsligt stöd för vidarebehandling av inhämtad information på fem särskilt angivna områden. Behandling av personuppgifter på dessa områden har således genom denna bestämmelse uttryckligt rättsligt stöd (preciserad finalitet) utöver vad som framgår av den allmänt formulerade bestämmelsen i 2 kap. 11 § andra stycket (finalitetsprincipen).

Utvecklingsverksamhet

4 §

Om det är nödvändigt för försvarsunderrättelseverksamheten får Försvarets radioanstalt behandla personuppgifter för att

1. följa förändringar i signalmiljön i omvärlden, den tekniska utvecklingen och signalskyddet, och

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

Paragrafen behandlas i avsnitt 6.3.7.

Paragrafen anger de ändamål för vilka personuppgifter får behandlas hos Försvarets radioanstalt i sådan utvecklingsverksamhet som bedrivs i syfte att skapa förutsättningar för försvarsunderrättelseverksamheten. Motsvarande ändamål finns i 2 § tredje stycket lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet.

5 §

Personuppgifter som behandlas med stöd av 4 § får även behandlas om det är nödvändigt för att tillhandahålla information som behövs

1. med anledning av samverkan med annan avseende utvecklingsverksamhet,

2. med anledning av samarbete om utvecklingsverksamhet med andra länder eller internationella organisationer enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet,

3. i försvarsunderrättelseverksamheten för de ändamål som anges i 1 och 2 §§,

4. i informationssäkerhetsverksamhet för de ändamål som anges i 6 §, eller

5. för att biträda andra myndigheter i den utsträckning det följer av lag eller förordning eller om regeringen i ett enskilt fall beslutar om det.

Bestämmelsen behandlas i avsnitt 6.3.7.

På samma sätt som 2 kap. 3 § innebär rättsligt stöd för vidarebehandling av uppgifter inom försvarsunderrättelseverksamheten, innebär denna bestämmelse rättsligt stöd för vidarebehandling av uppgifter inom utvecklingsverksamheten på fem särskilt angivna områden (preciserad finalitet). Paragrafen ger således stöd för behandling utöver den allmänt formulerade bestämmelsen i 2 kap. 11 andra stycket (finalitetsprincipen).

Informationssäkerhetsverksamhet

6 §

Personuppgifter får behandlas i Försvarets radioanstalts informationssäkerhetsverksamhet om det är nödvändigt för att kunna skydda den egna myndigheten eller för att kunna stödja andra verksamheter som är av betydelse för Sveriges säkerhet. Uppgiften att lämna stöd till andra verksamheter ska följa av lag eller förordning eller regeringsbeslut i ett enskilt fall.

Paragrafen behandlas i avsnitt 6.3.8.

Paragrafen utgör rättslig grund för behandling av personuppgifter i Försvarets radioanstalts informationssäkerhetsverksamhet. Behandling får ske om det är nödvändigt för att kunna skydda den egna myndigheten eller för att kunna stödja andra verksamheter som är av betydelse för Sveriges säkerhet. Försvarets radioanstalts uppdrag att vara statens resurs för teknisk informationssäkerhet och stöd för myndigheter och statligt ägda bolag på informationssäkerhetsområdet och ha hög kompetens framgår av 4 § förordningen med instruktion för Försvarets radioanstalt. Verksamheten bedrivs bl.a. med stöd av det tekniska detekterings- och varningssystemet (TDV) som beskrivs i avsnitt 3.3.6.

7 §

Personuppgifter som behandlas med stöd av 6 § får även behandlas om det är nödvändigt för att tillhandahålla information som behövs

1. i verksamhet hos den som tar emot uppgifter om informationssäkerhet,

2. med anledning av samverkan med andra som verkar på informationssäkerhetsområdet såväl inom som utom landet i den utsträckning det följer av lag eller förordning eller om regeringen i ett enskilt fall beslutar om det,

3. i försvarsunderrättelseverksamheten för de ändamål som anges i 1 § andra stycket 5 och 7 lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet, eller

4. i utvecklingsverksamheten för de ändamål som anges i 4 §.

Paragrafen behandlas i avsnitt 6.3.8.

På samma sätt som 2 kap. 3 § innebär rättsligt stöd för vidarebehandling av uppgifter inom försvarsunderrättelseverksamheten och 2 kap. 5 § inom utvecklingsverksamheten, innebär denna bestämmelse rättsligt stöd för vidarebehandling av uppgifter inom informationssäkerhetsverksamheten på fyra särskilt angivna områden (preciserad finalitet). Paragrafen ger således stöd för behandling utöver den allmänt formulerade bestämmelsen i 2 kap. 11 andra stycket (finalitetsprincipen).

Övriga rättsliga grunder

8 §

Personuppgifter som utgör allmänt tillgänglig information får behandlas av Försvarets radioanstalt om det är nödvändigt för de ändamål som anges i 1, 2, 4 och 6 §§.

Bestämmelsen behandlas i avsnitt 6.3.9.

För att kunna bedriva en effektiv försvarsunderrättelseverksamhet behöver Försvarets radioanstalt, utöver den information som den inhämtar genom signalspaning, också ha god tillgång till allmänt tillgänglig information. Därigenom kan den på hemligt sätt inhämtade informationen på ett bättre sätt än annars sättas in i sitt rätta sammanhang. Av intresse här är information som utgörs av personuppgifter som kan påträffas vid sökning på internet eller vid sökningar i öppna databaser. Uppgifterna kan vara gratis eller tillgängliga på kommersiell grund. Gemensamt för dem är att de är publikt tillgängliga. Det kan röra sig om uppgifter som t.ex. en abonnent på ett eller annat sätt har samtyckt att uppgifterna finns med i elektroniska telefonkataloger eller förteckningar över ip-adresser i olika länder. I stället för att myndigheten exponerar sig kan databaserna anskaffas och läggas upp som referensdatabaser hos myndigheten där den kan göra sökningar.

9 §

Försvarets radioanstalt får behandla personuppgifter för vetenskapliga, statistiska eller historiska ändamål inom denna lags tillämpningsområde.

Bestämmelsen behandlas i avsnitt 6.3.10.

Genom bestämmelsen ges Försvarets radioanstalt möjlighet att behandla personuppgifter för historiska, statistiska eller vetenskapliga ändamål.

10 §

Försvarets radioanstalt får behandla personuppgifter för att kunna tillgodose enskildas behov av information enligt 5 kap. och kunna lämna information vid tillsyn eller kontroll.

Bestämmelsen behandlas i avsnitt 6.3.11.

Sökningar i uppgiftssamlingar och sammanställningar av uppgifter som är nödvändig för att Försvarets radioanstalt ska kunna tillmötesgå tillsynsmyndighetens och kontrollmyndighetens behov innebär att personuppgifter behandlas. Bestämmelsen utgör rättslig grund för denna personuppgiftsbehandling samt för den personuppgiftsbehandling som krävs för att tillmötesgå enskildas rätt till information enligt 5 kap. Enskildas rättigheter behandlas vidare i avsnitt 6.7.3. Tillsynsmyndighetens verksamhet behandlas i avsnitt 6.8.

Grundläggande krav

Ändamål

11 §

Personuppgifter får bara behandlas för särskilda, uttryckligt angivna och berättigade ändamål.

Personuppgifter får inte behandlas för något ändamål som är oförenligt med det ändamål för vilket personuppgifterna ursprungligen behandlades.

Bestämmelsen behandlas i avsnitt 6.4.1.

Paragrafen sätter, tillsammans med bestämmelserna i 12 och 13 §§, vissa ramar för Försvarets radioanstalts personuppgiftsbehandling inom lagens verksamhetsområden.

Bestämmelsen motsvarar 2 kap. 12 § i förslaget till lag om behandling av personuppgifter vid Försvarsmakten. För en kommentar hänvisas till den bestämmelsen.

Författningsenlig och korrekt behandling

12 §

Personuppgifter ska behandlas författningsenligt och på ett korrekt sätt.

Bestämmelsen motsvarar 2 kap. 13 § i förslaget till lag om behandling av personuppgifter vid Försvarsmakten. För en kommentar hänvisas till den bestämmelsen.

Personuppgifternas kvalitet

13 §

Personuppgifter som behandlas ska vara adekvata och relevanta i förhållande till ändamålen med behandlingen och, om det är nödvändigt, uppdaterade.

Uppgifter som beskriver en persons utseende ska utformas på ett objektivt sätt med respekt för människovärdet.

Fler personuppgifter får inte behandlas än vad som är nödvändigt med hänsyn till ändamålen med behandlingen.

Bestämmelsen motsvarar 2 kap. 14 § i förslaget till lag om behandling av personuppgifter vid Försvarsmakten. För en kommentar hänvisas till den bestämmelsen.

Känsliga personuppgifter

14 §

Personuppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening eller som rör hälsa, sexualliv eller sexuell läggning får inte behandlas.

När uppgifter om en person behandlas får de dock kompletteras med sådana uppgifter som avses i första stycket, om det är absolut nödvändigt för syftet med behandlingen.

Bestämmelsen motsvarar 2 kap. 15 § i förslaget till lag om behandling av personuppgifter vid Försvarsmakten. För en kommentar hänvisas till den bestämmelsen.

15 §

Biometriska uppgifter får behandlas endast om det är absolut nödvändigt för ändamålet för behandlingen. Genetiska uppgifter får inte behandlas.

Bestämmelsen motsvarar 2 kap. 16 § i förslaget till lag om behandling av personuppgifter vid Försvarsmakten. För en kommentar hänvisas till den bestämmelsen.

16 §

Vid sökning får personuppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening eller som rör hälsa, sexualliv eller sexuell läggning användas som sökbegrepp om det är absolut nödvändigt för syftet med behandlingen. Detsamma gäller biometriska uppgifter.

Bestämmelsen motsvarar 2 kap. 17 § i förslaget till lag om behandling av personuppgifter vid Försvarsmakten. För en kommentar hänvisas till den bestämmelsen.

Om den som uppgifterna rör har offentliggjort uppgifterna

17 §

Utan hinder av vad som föreskrivs i 14 och 15 §§ får personuppgifter behandlas, om den som personuppgifterna rör på ett tydligt sätt offentliggjort uppgifterna.

Första stycket gäller inte genetiska uppgifter.

Bestämmelsen motsvarar 2 kap. 19 § i förslaget till lag om behandling av personuppgifter vid Försvarsmakten. För en kommentar hänvisas till den bestämmelsen.

Behandling av personuppgifter i vissa fall

18 §

Hantering av information som innebär behandling av personuppgifter ska inte anses oförenlig med bestämmelserna i 1, 4, 6, 8 och 11–15 §§ i det skede av behandlingen då det inte har kunnat fastställas vilka personuppgifter som informationen innehåller.

Bestämmelsen motsvarar 2 kap. 20 § i förslaget till lag om behandling av personuppgifter vid Försvarsmakten. För en kommentar hänvisas till den bestämmelsen.

Längsta tid som personuppgifter får behandlas

19 §

Personuppgifter som behandlas automatiserat får inte behandlas under längre tid än vad som behövs för något eller några av de ändamål som anges i 1–10 §§.

Regeringen eller den myndighet regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter eller i ett enskilt fall besluta att personuppgifter får behandlas under endast viss tid eller bevaras för historiska, statistiska eller vetenskapliga ändamål.

Bestämmelsen motsvarar 2 kap. 21 § i förslaget till lag om behandling av personuppgifter vid Försvarsmakten. För en kommentar hänvisas till den bestämmelsen.

Utlämnande av personuppgifter

20 §

Personuppgifter som behandlas med stöd av denna lag får föras över till en utländsk underrättelse- eller säkerhetstjänst, en utländsk organisation inom informationssäkerhetsområdet eller en internationell organisation endast om sekretess inte hindrar det och det är nödvändigt för att Försvarets radioanstalt ska kunna fullgöra sina uppgifter inom ramen för internationellt försvarsunderrättelse- och säkerhetssamarbete.

Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter eller i enskilt fall besluta att överföring får ske även i andra fall då det är nödvändigt för verksamheten vid Försvarets radioanstalt.

Enligt paragrafen, som behandlas i avsnitt 6.4.8, får personuppgifter föras över till en utländsk underrättelse- eller säkerhetstjänst, en utländsk organisation inom informationssäkerhetsområdet eller en internationell organisation endast om sekretess inte hindrar det och det är nödvändigt för att Försvarets radioanstalt ska kunna fullgöra sina uppgifter inom ramen för internationellt försvarsunderrättelse- och säkerhetssamarbete.

Paragrafen är ägnad att uppfylla de krav på nationell lagstiftning som dataskyddskonventionen ställer när det gäller överföring av personuppgifter till andra länder. Huruvida ett utlämnande ska ske eller inte måste i sin helhet avgöras efter en sekretessprövning och försvars- och säkerhetspolitiska överväganden.

Av bestämmelsen framgår vidare att begränsningarna av möjligheterna till överföring gäller såvida inte regeringen har meddelat föreskrifter eller beslut i enskilda fall om att överföring får ske även i andra fall då det är nödvändigt för verksamheten vid Försvarets radioanstalt.

21 §

Personuppgifter får lämnas ut elektroniskt på annat sätt än genom direktåtkomst om regeringen har meddelat föreskrifter eller särskilt beslutat om det.

Elektroniskt utlämnande genom direktåtkomst är tillåtet bara i den utsträckning som anges i 3 kap. 2–6 §§.

Paragrafen behandlas i avsnitt 6.4.8.

Enligt *första stycket* får personuppgifter får lämnas ut elektroniskt på annat sätt än genom direktåtkomst om regeringen har meddelat föreskrifter eller särskilt beslutat om det.

3 kap. Gemensamt tillgängliga uppgifter

Personuppgifter som får göras gemensamt tillgängliga

1 §

Personuppgifter får göras gemensamt tillgängliga och behandlas i uppgiftssamlingar om det behövs för något av de ändamål som anges i 2 kap. 1–10 §§. Personuppgifter som endast ett fåtal personer har tillgång till anses inte som gemensamt tillgängliga.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter eller besluta i enskilda fall vilka uppgiftssamlingar som får finnas och vilka uppgifter som får behandlas i respektive uppgiftssamling.

I paragrafen, behandlas i avsnitt 6.5.1, anges i *första stycket* genom en hänvisning till lagens syften vilka personuppgifter som får göras gemensamt tillgängliga och behandlas i uppgiftssamlingar. Genom hänvisningen omfattas även informationssäkerhetsverksamheten.

En grundläggande förutsättning för att personuppgifter ska anses vara gemensamt tillgängliga är att de kan användas gemensamt av flera, dvs. att fler än en person har åtkomst till uppgifterna. Uppgifter som endast ett fåtal personer har rätt att ta del av bör dock inte anses som gemensamt tillgängliga. Vad som utgör en uppgiftssamling definieras i 1 kap. 8 §.

Av *andra stycket* framgår att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter eller besluta i enskilda

fall vilka uppgiftssamlingar som får finnas och vilka uppgifter som får behandlas i respektive uppgiftssamling.

I förslaget till förordning finns i 3 kap. 1–7 §§ bestämmelser om uppgiftssamlingar för råmaterial, analyser, underrättelser, information om signalmiljön, företeelser mot vilka signalspaningen inriktas, information om teknik- och metodutveckling och signalskydd.

Direktåtkomst

Försvarsunderrättelseverksamhet

2 §

Trots sekretess enligt 38 kap. 4 § offentlighets- och sekretesslagen (2009:400) får Säkerhetspolisen och Försvarsmakten medges direktåtkomst till personuppgifter som utgör analysresultat inom försvarsunderrättelseverksamheten och som finns i uppgiftssamlingar.

Paragrafen, som behandlas i avsnitt 6.5.3, motsvarar 3 kap. 2 § i förslaget till lag om behandling av personuppgifter vid Försvarsmakten. För en kommentar hänvisas till den bestämmelsen.

Direktåtkomst enligt bestämmelsen är begränsad till personuppgifter som utgör analysresultat inom försvarsunderrättelseverksamheten och som finns i uppgiftssamlingar.

3 §

Om det behövs för samarbetet mot terrorism eller för annat internationellt säkerhetssamarbete får, i den utsträckning det följer av lag eller förordning eller om regeringen i ett enskilt fall beslutar om det, en utländsk underrättelse- eller säkerhetstjänst medges direktåtkomst till personuppgifter som behandlas med stöd av 2 kap. 1 § och som finns i uppgiftssamlingar.

Paragrafen motsvarar 3 kap. 3 § i förslaget till lag om behandling av personuppgifter vid Försvarsmakten. För en kommentar hänvisas till den bestämmelsen.

Informationssäkerhetsverksamhet

4 §

Om det behövs för samarbetet mot it-relaterade hot mot samhällsviktiga system får, i den utsträckning det följer av lag eller förordning eller om regeringen i ett enskilt fall beslutar om det, en utländsk organisation inom informationssäkerhetsområdet medges direktåtkomst till personuppgifter som behandlas med stöd av 2 kap. 6 § och som finns i uppgiftssamlingar.

Paragrafen behandlas i avsnitt 6.5.3.

Direktåtkomst för de områden som omfattas av bestämmelsen är begränsad till personuppgifter som behandlas inom Försvarets radioanstalts informationssäkerhetsverksamhet och som finns i uppgiftssamlingar.

Direktåtkomst i andra fall

5 §

Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter eller särskilt beslut om vilka som i andra fall än i 2–4 §§ får ha direktåtkomst till uppgiftssamlingar.

Paragrafen, som behandlas i avsnitt 6.5.3, är en upplysningsföreskrift om att regeringen kan meddela föreskrifter eller i ett enskilt fall besluta att direktåtkomst får medges i andra fall än de som anges i 2–4 §§.

Övriga bestämmelser

6 §

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela

1. ytterligare föreskrifter eller beslut i enskilda fall om omfattningen av direktåtkomsten, och

2. föreskrifter om behörighet och säkerhet vid sådan åtkomst.

Paragrafen, som behandlas i avsnitt 6.5.3, är en upplysningsföreskrift om att regeringen, eller den myndighet som regeringen bestämmer, kan meddela ytterligare föreskrifter eller beslut i enskilda fall om omfattningen av direktåtkomsten, och föreskrifter om behörighet och säkerhet vid sådan åtkomst.

4 kap. Skyldighet som personuppgiftsansvarig

Åtgärder för att säkerställa författningsenlig behandling

1 §

Försvarets radioanstalt ska, genom lämpliga tekniska och organisatoriska åtgärder, säkerställa att behandlingen av personuppgifter är författningsenlig och skydda rättigheterna för dem som uppgifterna rör.

Bestämmelsen motsvarar 4 kap. 1 § i förslaget till lag om behandling av personuppgifter vid Försvarsmakten. För en kommentar hänvisas till den bestämmelsen.

2 §

Försvarets radioanstalt ska säkerställa att det i uppgiftsamlingar förs loggar över personuppgiftsbehandling. Regeringen eller den myndighet regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om loggar.

Bestämmelsen motsvarar 4 kap. 2 § i förslaget till lag om behandling av personuppgifter vid Försvarsmakten, med den skillnaden att bestämmelsen för Försvarets radioanstalt avser uppgiftssamlingar. För en kommentar hänvisas till bestämmelsen i lag om behandling av personuppgifter vid Försvarsmakten.

3 §

Tillgången till personuppgifter ska alltid begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter.

Bestämmelsen motsvarar 4 kap. 3 § i förslaget till lag om behandling av personuppgifter vid Försvarsmakten. För en kommentar hänvisas till den bestämmelsen.

Säkerheten för personuppgifter

4 §

Försvarets radioanstalt ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas, särskilt mot obehörig eller otillåten behandling eller förstöring och mot förlust eller annan oavsiktlig skada.

Bestämmelsen motsvarar 4 kap. 4 § i förslaget till lag om behandling av personuppgifter vid Försvarsmakten. För en kommentar hänvisas till den bestämmelsen.

Dataskyddsombud

5 §

Försvarets radioanstalt ska inom myndigheten utse ett eller flera dataskyddsombud och anmäla dessa till tillsynsmyndigheten när dataskyddsombud utses och entledigas.

Bestämmelsen motsvarar 4 kap. 5 § i förslaget till lag om behandling av personuppgifter vid Försvarsmakten. För en kommentar hänvisas till den bestämmelsen.

6 §

Dataskyddsombudet ska

1. självständigt kontrollera att Försvarets radioanstalt behandlar personuppgifter författningsenligt och på ett korrekt sätt och i övrigt fullgör sina skyldigheter,

2. informera och ge råd till Försvarets radioanstalt och till dem som behandlar personuppgifter under myndighetens ledning om deras skyldigheter vid behandling av personuppgifter,

3. samråda med tillsynsmyndigheten, och

4. föra en förteckning över de kategorier av behandlingar som Försvarets radioanstalt ansvarar för och som är helt eller delvis automatiserade.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om vad en förteckning som avses i första stycket 4 ska innehålla.

Om Försvarets radioanstalt bryter mot de bestämmelser som gäller för behandlingen av personuppgifter och rättelse inte vidtas, ska dataskyddsombudet anmäla det till tillsynsmyndigheten.

Bestämmelsen motsvarar 4 kap. 6 § i förslaget till lag om behandling av personuppgifter vid Försvarsmakten. För en kommentar hänvisas till den bestämmelsen.

Personuppgiftsbiträden

7 §

Försvarets radioanstalt får, om det är lämpligt, anlita personuppgiftsbiträden för behandling av personuppgifter på Försvarets radioanstalts vägnar. Innan ett personuppgiftsbiträde anlitas, ska Försvarets radioanstalt försäkra sig om att biträdet kommer att vidta de lämpliga tekniska och organisatoriska åtgärder som krävs för att behandlingen av personuppgifter ska vara författningsenlig och för att skydda rättigheterna för den som uppgifterna rör.

Bestämmelsen motsvarar 4 kap. 7 § i förslaget till lag om behandling av personuppgifter vid Försvarsmakten. För en kommentar hänvisas till den bestämmelsen.

8 §

Personuppgiftsbiträdets behandling av personuppgifter ska regleras i ett skriftligt avtal eller annan skriftlig överenskommelse.

Bestämmelsen motsvarar 4 kap. 8 § i förslaget till lag om behandling av personuppgifter vid Försvarsmakten. För en kommentar hänvisas till den bestämmelsen.

9 §

Ett personuppgiftsbiträde får inte anlita ett annat personuppgiftsbiträde utan skriftligt tillstånd av Försvarets radioanstalt.

Bestämmelsen motsvarar 4 kap. 9 § i förslaget till lag om behandling av personuppgifter vid Försvarsmakten. För en kommentar hänvisas till den bestämmelsen.

10 §

Ett personuppgiftsbiträde eller den eller de personer som arbetar under biträdets eller Försvarets radioanstalts ledning ska behandla personuppgifter i enlighet med instruktioner från Försvarets radioanstalt.

Om ett personuppgiftsbiträde, i strid med Försvarets radioanstalts instruktioner, bestämmer ändamålen med och medlen för behandlingen, ska biträdet anses vara personuppgiftsansvarig enligt denna lag för den behandlingen.

Bestämmelsen motsvarar 4 kap. 10 § i förslaget till lag om behandling av personuppgifter vid Försvarsmakten. För en kommentar hänvisas till den bestämmelsen.

11 §

Det som sägs om Försvarets radioanstalts skyldigheter i 2–4 §§ gäller även för personuppgiftsbiträden som Försvarets radioanstalt anlitar.

Bestämmelsen motsvarar 4 kap. 11 § i förslaget till lag om behandling av personuppgifter vid Försvarsmakten. För en kommentar hänvisas till den bestämmelsen.

5 kap. Enskildas rättigheter

Rätten till information

Allmän information

1 §

Försvarets radioanstalt ska göra följande allmänna information tillgänglig.

1. Myndighetens identitet och kontaktuppgifter.

2. Uppgifter om dataskyddsombudet.

3. Ändamålen med behandlingen.

4. Rätten enligt 2 § att begära att få information om behandling av personuppgifter och att få del av dem.

5. Rätten att begära rättelse, radering eller begränsning av behandlingen enligt 5 §.

Bestämmelsen motsvarar 5 kap. 1 § i förslaget till lag om behandling av personuppgifter vid Försvarsmakten. För en kommentar hänvisas till den bestämmelsen.

Information som ska lämnas efter begäran

2 §

Försvarets radioanstalt är skyldig att utan onödigt dröjsmål en gång per kalenderår till den som begär det lämna skriftligt besked om personuppgifter som rör honom eller henne behandlas. Behandlas sådana uppgifter ska sökanden få del av dem och få följande skriftliga information.

1. Vilka personuppgifter om den sökande som behandlas.

2. Varifrån personuppgifterna kommer.

3. Den rättsliga grunden för behandlingen.

4. Ändamålen med behandlingen.

5. Mottagare eller kategorier av mottagare av personuppgifterna, även i annat land eller internationella organisationer.

6. Hur länge personuppgifterna får behandlas eller, om det inte är möjligt att ange, kriterierna för att fastställa det.

7. Rätten att begära rättelse, radering eller begränsning av behandlingen enligt 5 §.

Utlämnande enligt första stycket behöver inte omfatta personuppgifter som sökanden har tagit del av, om inte han eller hon begär det. Det ska dock framgå av informationen att personuppgifterna i fråga behandlas.

En ansökan enligt första stycket ska göras skriftligen hos Försvarets radioanstalt och vara undertecknad av den sökande själv. Information enligt första stycket ska 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.

Bestämmelsen motsvarar 5 kap. 3 § i förslaget till lag om behandling av personuppgifter vid Försvarsmakten. För en kommentar hänvisas till den bestämmelsen.

Begränsning av rätten till information

3 §

Informationsskyldigheten i 2 § gäller inte i den utsträckning sekretess hindrar att uppgifterna lämnas ut.

Om förutsättningarna i första stycket är uppfyllda, är Försvarets radioanstalt inte skyldig att lämna ut skälen för beslut enligt första stycket eller beslut i fråga om rättelse, radering eller begränsning av behandlingen enligt 5 §.

Bestämmelsen motsvarar 5 kap. 4 § i förslaget till lag om behandling av personuppgifter vid Försvarsmakten. För en kommentar hänvisas till den bestämmelsen.

4 §

Informationsskyldigheten i 2 § gäller inte personuppgifter i löpande text som inte fått sin slutliga utformning när begäran gjordes eller som utgör minnesanteckning eller liknande.

Informationsskyldigheten gäller dock om uppgifterna har lämnats ut till tredje part, behandlas enbart för vetenskapliga, statistiska eller historiska ändamål eller arkivändamål av allmänt intresse eller, när det gäller löpande text som inte fått sin slutliga utformning, om uppgifterna har behandlats längre än ett år.

Bestämmelsen motsvarar 5 kap. 5 § i förslaget till lag om behandling av personuppgifter vid Försvarsmakten. För en kommentar hänvisas till den bestämmelsen.

Rätten till rättelse, radering och begränsning av behandlingen

5 §

Försvarets radioanstalt ska på begäran av den som personuppgiften rör snarast rätta, radera eller begränsa sådana personuppgifter som inte har behandlats i enlighet med denna lag eller föreskrifter som har meddelats med stöd av lagen.

Försvarets radioanstalt ska också underrätta tredje part till vilken uppgifterna har lämnats ut om åtgärden, om den som personuppgiften rör begär det eller om en mera betydande skada eller olägenhet för denne skulle kunna undvikas genom en underrättelse.

Någon underrättelse behöver dock inte lämnas, om sekretess hindrar det eller detta är omöjligt eller skulle innebära en oproportionerligt stor arbetsinsats.

Bestämmelsen motsvarar 5 kap. 6 § i förslaget till lag om behandling av personuppgifter vid Försvarsmakten. För en kommentar hänvisas till den bestämmelsen.

Avgiftsfri information

6 §

Information enligt 1 § ska lämnas utan avgift.

Information och uppgifter enligt 2 § ska lämnas utan avgift en gång per kalenderår. Om någon begär information och uppgifter enligt 2 § oftare än en gång per kalenderår, får Försvarets radioanstalt avslå begäran.

Bestämmelsen motsvarar 5 kap. 7 § i förslaget till lag om behandling av personuppgifter vid Försvarsmakten. För en kommentar hänvisas till den bestämmelsen.

6 kap. Tillsyn

Tillsyn över personuppgiftsbehandlingen

1 §

Den myndighet som regeringen bestämmer ska utöva allmän tillsyn över Försvarets radioanstalts behandling av personuppgifter enligt denna lag.

Tillsynsmyndigheten ska ge råd och stöd till Försvarets radioanstalt om myndighetens skyldigheter enligt lag eller annan författning eller när det i övrigt är påkallat.

Bestämmelsen motsvarar 6 kap. 1 § i förslaget till lag om behandling av personuppgifter vid Försvarsmakten. För en kommentar hänvisas till den bestämmelsen.

2 §

I lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet finns det särskilda bestämmelser om kontroll som rör Försvarets radioanstalts behandling av personuppgifter i försvarsunderrättelse- och utvecklingsverksamheten.

Paragrafen behandlas i avsnitt 6.8.1 och upplyser om att det i lagen om signalspaning i försvarsunderrättelseverksamhet finns särskilda bestämmelser om kontroll. Enligt 10 § nämnda lag ska kontrollen

särskilt avse granskning av sökbegrepp, förstöring av uppgifter samt rapportering.

Befogenheter

Utredningsbefogenheter

3 §

Tillsynsmyndigheten har rätt att av Försvarets radioanstalt eller ett personuppgiftsbiträde på begäran få

1. tillgång till personuppgifter som behandlas,

2. upplysningar om och dokumentation av behandlingen av personuppgifter och säkerhets- och skyddsåtgärder,

3. tillträde till sådana lokaler som har anknytning till behandling av personuppgifter och tillgång till utrustning och andra medel för behandling av personuppgifter, och

4. det biträde och annan information som behövs för tillsynen.

Bestämmelsen motsvarar 6 kap. 2 § i förslaget till lag om behandling av personuppgifter vid Försvarsmakten. För en kommentar hänvisas till den bestämmelsen.

Förebyggande befogenheter

4 §

Om tillsynsmyndigheten bedömer att det finns risk för att personuppgifter kan komma att behandlas i strid med lag eller annan författning, ska myndigheten genom råd, rekommendationer eller påpekanden försöka förmå Försvarets radioanstalt eller personuppgiftsbiträdet att vidta åtgärder för att minska den risken.

Tillsynsmyndigheten får utfärda en skriftlig varning för att planerad behandling av personuppgifter riskerar att stå i strid med lag eller annan författning. Detsamma gäller om pågående behandling riskerar att stå i strid med lag eller annan författning.

Bestämmelsen motsvarar 6 kap. 3 § i förslaget till lag om behandling av personuppgifter vid Försvarsmakten. För en kommentar hänvisas till den bestämmelsen.

Korrigerande befogenheter

5 §

Om tillsynsmyndigheten konstaterar att personuppgifter behandlas i strid med lag eller annan författning, eller att Försvarets radioanstalt eller ett personuppgiftsbiträde annars inte fullgör sina skyldigheter, får tillsynsmyndigheten

1. genom sådana åtgärder som anges i 4 § första stycket försöka förmå Försvarets radioanstalt eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsenlig eller att uppfylla andra skyldigheter, eller

2. förelägga Försvarets radioanstalt eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsenlig eller att fullgöra andra skyldigheter.

Om ett föreläggande utfärdas ska det av föreläggandet framgå när åtgärderna senast ska vara genomförda och, om det är lämpligt, vilka åtgärder som ska vidtas.

Bestämmelsen motsvarar 6 kap. 4 § i förslaget till lag om behandling av personuppgifter vid Försvarsmakten. För en kommentar hänvisas till den bestämmelsen.

7 kap. Skadestånd och överklagande

Skadestånd

1 §

Den personuppgiftsansvarige ska ersätta den som personuppgiften rör för skada och kränkning av den personliga integriteten som orsakats av behandling av personuppgifter i strid med denna lag, eller föreskrifter som har meddelats i anslutning till den.

Ersättningsskyldigheten kan i den utsträckning det är skäligt, jämkas om den personuppgiftsansvarige visar att felet inte berodde på denne.

Bestämmelsen motsvarar 7 kap. 1 § i förslaget till lag om behandling av personuppgifter vid Försvarsmakten. För en kommentar hänvisas till den bestämmelsen.

Överklagande

2 §

Försvarets radioanstalts beslut om information som ska lämnas enligt 5 kap. 2 § och om rättelse och underrättelse till tredje part enligt 5 kap. 5 § får överklagas hos allmän förvaltningsdomstol. Andra beslut enligt denna lag får inte överklagas.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Bestämmelsen motsvarar 7 kap. 2 § i förslaget till lag om behandling av personuppgifter vid Försvarsmakten. För en kommentar hänvisas till den bestämmelsen.

3 §

Av 6 kap. 8 § offentlighets- och sekretesslagen (2009:400) följer att beslut om sekretess överklagas till kammarrätt.

Paragrafen upplyser om att beslut i frågor om sekretess överklagas direkt till kammarrätt som första överprövningsinstans.

8.3 Förslaget till lag om ändring i lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning

1 kap.

3 §

Bestämmelserna i 2 § gäller inte i verksamhet som omfattas av

1. lagen (2019:000) om behandling av personuppgifter vid Försvarsmakten,

2. lagen (2019:000) om behandling av personuppgifter vid Försvarets radioanstalt, eller

3. 6 kap. polisdatalagen (2010:361).

Paragrafen behandlas i avsnitt 6.12.1 och innebär att hänvisningarna till FM-PuL och FRA-PuL ersätts med hänvisningar till lagen om behandling av personuppgifter vid Försvarsmakten respektive lagen om behandling av personuppgifter vid Försvarets radioanstalt.

8.4 Förslaget till lag om ändring i brottsdatalagen (2018:1177)

1 kap.

4 §

Lagen gäller inte vid Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet eller om Polismyndigheten har övertagit en arbetsuppgift som rör nationell säkerhet från Säkerhetspolisen.

Lagen gäller inte heller i sådan verksamhet som omfattas av lagen (2019:000) om behandling av personuppgifter vid Försvarsmakten.

Paragrafen behandlas i avsnitt 6.12.2 och innebär att hänvisningen till FM-PuL i andra stycket ersätts med en hänvisning till lagen om behandling av personuppgifter vid Försvarsmakten.

8.5 Förslaget till lag om ändring i lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet

2 a §

Inhämtning får inte avse signaler mellan en avsändare och mottagare som båda befinner sig i Sverige. Om sådana signaler inte kan avskiljas redan vid inhämtningen, ska upptagningen eller uppteckningen förstöras så snart det står klart att sådana signaler har inhämtats.

Första stycket tillämpas inte i fråga om signaler som utväxlas autonomt mellan tekniska system i sådana fall där signalerna inte innehåller personuppgifter. Första stycket tillämpas inte heller i fråga om övriga signaler mellan sändare och mottagare på utländska statsfartyg, statsluftfartyg eller militära fordon.

Paragrafen behandlas i avsnitt 6.12.3. I andra stycket första meningen har införts ett nytt undantag från bestämmelserna i första stycket. Det nya undantaget avser signaler som utväxlas autonomt mellan tekniska system i sådana fall där signalerna inte innehåller personuppgifter.

12 a §

I lagen (2019:000) om behandling av personuppgifter vid Försvarets radioanstalt finns ytterligare bestämmelser om behandlingen av inhämtade personuppgifter.

Paragrafen behandlas i avsnitt 6.12.3 och innebär att hänvisningen till FRA-PuL ersätts med en hänvisning till den föreslagna lagen om behandling av personuppgifter vid Försvarets radioanstalt.

Kommittédirektiv 2017:42

Behandlingen av personuppgifter inom Försvarsmakten och Försvarets radioanstalt

Beslut vid regeringssammanträde den 27 april 2017

Sammanfattning

En särskild utredare ska göra en översyn av den lagstiftning som gäller för personuppgiftsbehandling inom Försvarsmakten och Försvarets radioanstalt. Syftet med uppdraget är att säkerställa att lagstiftningen är anpassad till den tekniska och legala utvecklingen.

Utredaren ska bl.a.

- analysera om rådande lagstiftning är ändamålsenlig för Försvarsmaktens och Försvarets radioanstalts verksamheter och om den är tillräcklig i fråga om skyddet för enskildas personliga integritet,
- särskilt utreda hur personuppgifter behandlas i Försvarets radioanstalt i samband med att myndigheten stödjer andra myndigheter och statligt ägda bolag inom informationssäkerhetsområdet, och
- lämna de författningsförslag som behövs och är lämpliga.

Uppdraget ska redovisas senast den 31 maj 2018.

Grundläggande bestämmelser om skyddet av personuppgifter

En väl avvägd balans är nödvändig mellan å ena sidan skyddet för den personliga integriteten och å andra sidan upprätthållandet av statens säkerhet. Den snabba tekniska utvecklingen skapar möjligheter att på ett effektivt sätt inhämta information som är av betydelse för att

kunna skydda landet mot yttre hot, men innebär samtidigt utmaningar för skyddet av den personliga integriteten. Intrång i den personliga integriteten måste alltid stå i rimlig proportion till det intresse som ska tillgodoses med behandlingen av personuppgifterna.

Grundläggande bestämmelser till skydd för den personliga integriteten finns i regeringsformen. I 1 kap. 2 § första stycket slås det fast att den offentliga makten ska utövas med respekt bl.a. för den enskilda människans frihet och i fjärde stycket anges bl.a. att det allmänna ska värna den enskildes privatliv och familjeliv. Enligt 2 kap. 6 § andra stycket är var och en skyddad gentemot det allmänna mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Inskränkningar i det grundlagsfästa skyddet kan endast göras genom lag och bara under de förutsättningar som anges i 2 kap. 20–22 §§ regeringsformen.

Enligt artikel 8 i den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) har var och en rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. Med detta avses bl.a. skyddet av personuppgifter. Rättigheten är dock inte absolut. Inskränkningar får göras med stöd av lag och om det är nödvändigt i ett demokratiskt samhälle med hänsyn till vissa särskilt angivna ändamål, bl.a. statens säkerhet och den allmänna säkerheten. Av 2 kap. 19 § regeringsformen följer att en lag eller annan föreskrift inte får meddelas i strid med Sveriges åtaganden på grund av konventionen.

Den europeiska konventionen om skydd för enskilda vid automatisk databehandling av personuppgifter, den s.k. dataskyddskonventionen, kan ses som en precisering av skyddet för enskilda enligt artikel 8 i Europakonventionen i fråga om behandlingen av personuppgifter. Konventionen och dess tilläggsprotokoll har ett generellt tillämpningsområde och kompletteras av ett antal rekommendationer som antagits av ministerkommittén och som handlar om hur personuppgifter bör behandlas inom olika områden. Sverige har, i likhet med övriga medlemsstater i EU, anslutit sig till dataskyddskonventionen. En översyn av konventionen pågår inom Europarådet.

I Europeiska unionens stadga om de grundläggande rättigheterna bekräftas de rättigheter som har sin grund i medlemsstaternas gemensamma författningstraditioner och internationella förpliktelser, Europakonventionen, unionens och Europarådets sociala stadgor samt

rättspraxis vid Europeiska unionens domstol och Europeiska domstolen för de mänskliga rättigheterna. Artikel 7 i stadgan anger att var och en har rätt till respekt för sitt privatliv och familjeliv, sin bostad och sina kommunikationer. Artikel 8 reglerar skydd av personuppgifter. Enligt artikeln har var och en rätt till skydd av de personuppgifter som rör honom eller henne. Sådana uppgifter ska behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund. Var och en har rätt att få tillgång till insamlade uppgifter som rör honom eller henne och att få dem rättade. En oberoende myndighet ska kontrollera att reglerna följs.

EU-regleringen och dess svenska genomförande

EU:s dataskyddsdirektiv

Den allmänna regleringen om behandling av personuppgifter inom EU finns i dag i 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 behandling av det fria flödet av sådana uppgifter (dataskyddsdirektivet).

Dataskyddsdirektivet gäller inte för behandling av personuppgifter på områden som faller utanför gemenskapsrätten, t.ex. försvar och statens säkerhet (artikel 3.2). Direktivet har genomförts i svensk rätt genom personuppgiftslagen (1998:204). Sverige valde i samband med att dataskyddsdirektivet genomfördes i svensk rätt att inte begränsa personuppgiftslagens tillämpningsområde, bl.a. med motiveringen att det är särskilt viktigt med ett starkt integritetsskydd när det gäller uppgifter inom all offentlig verksamhet. En annan motivering var att den valda lösningen garanterar att behovet av särregler i förhållande till personuppgiftslagen alltid övervägs noga i den ordning som krävs för författningsgivning (se prop. 1997/98:44 s. 40–41).

EU:s dataskyddsförordning

Den 27 april 2016 antogs Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana

uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), kallad dataskyddsförordningen. Förordningen utgör en ny generell reglering för personuppgiftsbehandling inom EU och kommer att ersätta det nuvarande dataskyddsdirektivet. Förordningen ska börja tillämpas den 25 maj 2018.

Dataskyddsförordningen baseras till stor del på dataskyddsdirektivets struktur och innehåll, men rymmer även en rad nyheter såsom en utökad informationsskyldighet, administrativa sanktionsavgifter och inrättandet av Europeiska dataskyddsstyrelsen. Dataskyddsförordningen är direkt tillämplig i medlemsstaterna, men den både förutsätter och möjliggör kompletterande nationella bestämmelser av olika slag. Behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av unionsrätten, t.ex. försvar och statens säkerhet, undantas från dataskyddsförordningens tillämpningsområde, på samma sätt som gäller för dataskyddsdirektivet. Förordningen ger också ett visst utrymme för medlemsstaterna att behålla eller införa mer specifika bestämmelser för sådan personuppgiftsbehandling som är nödvändig för att den personuppgiftsansvarige ska kunna uppfylla en rättslig skyldighet, utföra en arbetsuppgift av allmänt intresse eller behandla uppgifter i samband med myndighetsutövning (förordningens artikel 6.2).

Regeringen tillsatte den 25 februari 2016 en utredning som bl.a. ska undersöka vilka kompletterande nationella föreskrifter som dataskyddsförordningen kräver (Ju 2016:04). I utredningens direktiv anges att personuppgiftslagen och personuppgiftsförordningen (1998:1191) samt Datainspektionens föreskrifter i anslutning till denna reglering kommer att behöva upphävas. Uppdraget ska redovisas senast den 12 maj 2017.

Regeringen har även tillsatt en utredning som ska föreslå hur EU:s direktiv om skydd av personuppgifter vid brottsbekämpning, brottmålshantering och straffverkställighet ska genomföras i svensk rätt (Ju 2016:06). Uppdraget ska redovisas senast den 30 september 2017.

Uppdraget att se över den reglering som gäller vid behandling av personuppgifter inom Försvarsmakten och Försvarets radioanstalt

Myndigheternas verksamhet ska kunna bedrivas effektivt med rationellt datorstöd samtidigt som enskildas integritet värnas

Personuppgiftslagen är subsidiär vilket innebär att lagens bestämmelser inte ska tillämpas om det finns avvikande bestämmelser i en annan lag eller förordning. Det finns en stor mängd sådana bestämmelser i s.k. särskilda registerförfattningar.

På Försvarsmaktens verksamhetsområde finns lagen (2007:258) och förordningen (2007:260) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst. För stora delar av Försvarets radioanstalts verksamhet gäller lagen (2007:259) och förordningen (2007:261) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse och utvecklingsverksamhet. Lagarna är fristående i förhållande till personuppgiftslagen, men deras strukturer och materiella innehåll är till stor del inspirerade av den lagen.

Försvarsmakten och Försvarets radioanstalt behandlar även personuppgifter för andra syften än de som anges i nu nämnda lagar, t.ex. inom myndigheternas administrativa verksamhet. För sådan behandling av personuppgifter gäller personuppgiftslagen.

De särskilda lagarna om viss personuppgiftsbehandling inom Försvarsmakten och Försvarets radioanstalt tillkom 2007. Personuppgiftslagen kommer att ersättas av dataskyddsförordningen och nationella kompletterande bestämmelser. Det finns därför anledning att säkerställa att regleringen av all den personuppgiftsbehandling som sker inom Försvarsmakten och Försvarets radioanstalt är ändamålsenlig i förhållande till såväl ny övergripande reglering, den tekniska utvecklingen och myndigheternas verksamheter i övrigt. Utgångspunkten är att myndigheternas verksamheter ska kunna bedrivas effektivt med rationellt datorstöd samtidigt som enskildas personliga integritet värnas.

Utredaren ska därför

- översiktligt beskriva hur personuppgifter behandlas och vilken reglering som gäller för behandlingen inom Försvarsmakten och Försvarets radioanstalt,

- bedöma om den reglering som gäller vid behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst och i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet är ändamålsenligt utformad och tillräcklig när det gäller skyddet för enskildas personliga integritet,
- analysera vilket utrymme det finns för nationell reglering av den personuppgiftsbehandling i Försvarsmakten och Försvarets radioanstalt som i dag regleras i personuppgiftslagen, och utifrån den analysen bedöma om behandlingen helt eller delvis bör regleras särskilt, och
- lämna de författningsförslag som behövs och är lämpliga.

Hur bör personuppgiftsbehandlingen inom Försvarets radioanstalts arbete med informationssäkerhet regleras?

Försvarets radioanstalt ska ha hög teknisk kompetens inom informationssäkerhetsområdet och får, efter begäran, stödja andra statliga myndigheter och statligt ägda bolag som hanterar information som bedöms vara känslig från sårbarhets-, säkerhets- eller försvarspolitisk synpunkt. Försvarets radioanstalt gör detta bl.a. genom att på begäran av berörd myndighet eller berört bolag testa sårbarheten i myndighetens eller bolagets it-system. På grund av utvecklingen när det gäller avancerade it-angrepp har Försvarets radioanstalt på regeringens uppdrag tagit fram ett tekniskt detekterings- och varningssystem för att stärka informationssäkerheten vid de mest skyddsvärda verksamheterna bland statliga myndigheter och statligt ägda bolag.

Den personuppgiftsbehandling som kan uppkomma inom ramen för Försvarets radioanstalts arbete på informationssäkerhetsområdet, och som myndigheten ansvarar för, regleras av personuppgiftslagen. Som nämnts kommer lagen att upphävas och ersättas av dataskyddsförordningen med kompletterande nationella föreskrifter.

Utredaren ska därför

- närmare utreda hur personuppgifter behandlas inom Försvarets radioanstalt i samband med att myndigheten stödjer andra myndigheter och statligt ägda bolag inom informationssäkerhetsområdet,

- bedöma om regleringen för personuppgiftsbehandlingen i Försvarets radioanstalt är ändamålsenlig med hänsyn till verksamheten och skyddet för enskildas personliga integritet,
- analysera vilket utrymme det finns för en nationell reglering, och
- lämna lämpliga författningsförslag.

Konsekvensbeskrivningar

Utredaren ska bedöma de ekonomiska konsekvenserna av förslagen för det allmänna och för enskilda. Om förslagen kan förväntas leda till kostnadsökningar för det allmänna ska utredaren föreslå hur dessa ska finansieras. Utredaren ska också redovisa förslagens konsekvenser för den personliga integriteten och för eventuella verksamhetsmässiga konsekvenser.

Samråd och redovisning av uppdraget

När utredaren genomför uppdraget ska han eller hon särskilt höra Statens inspektion för försvarsunderrättelseverksamheten. Utredaren ska även, i den utsträckning som bedöms lämplig, ha en dialog med och inhämta upplysningar från övriga myndigheter och andra som kan vara berörda av aktuella frågor.

Utredaren ska hålla sig väl informerad om och beakta relevant arbete som bedrivs inom Regeringskansliet, utredningsväsendet och Europarådet. Detta innebär bl.a. att utredaren ska hålla sig informerad om arbetet med en ny säkerhetsskyddslag (SOU 2015:25), liksom det arbete som bedrivs i Integritetskommittén (Ju 2014:09), i Dataskyddsutredningen (Ju 2016:04), i utredningen om 2016 års dataskyddsdirektiv (Ju 2016:06), i utredningen om behandling av personuppgifter om totalförsvarspliktiga (Fö 2016:01), samt om den översyn som görs av dataskyddskonventionen.

Uppdraget ska redovisas senast den 31 maj 2018.

(Försvarsdepartementet)

Kommittédirektiv 2018:28

Tilläggsdirektiv till Utredningen behandlingen av personuppgifter inom Försvarsmakten och Försvarets radioanstalt (Fö 2017:03)

Beslut vid regeringssammanträde den 19 april 2018

Förlängd tid för uppdraget

Regeringen beslutade den 27 april 2017 kommittédirektiv om behandlingen av personuppgifter inom Försvarsmakten och Försvarets radioanstalt (dir. 2017:42). Enligt utredningens direktiv skulle uppdraget redovisas senast den 31 maj 2018.

Utredningstiden förlängs. Uppdraget ska i stället redovisas senast den 31 juli 2018.

(Försvarsdepartementet)

Statens offentliga utredningar 2018

Kronologisk förteckning

1. Ett reklamlandskap i förändring – konsumentskydd och tillsyn i en digitaliserad värld. Fi.
2. Stärkt straffrättsligt skydd för blåljusverksamhet och andra samhällsnyttiga funktioner. Ju.
3. En strategisk agenda för internationalisering. U.
4. Framtidens biobanker. S.
5. Vissa processuella frågor på socialförsäkringsområdet. S.
6. Grovt upphovsrättsbrott och grovt varumärkesbrott. Ju.
7. Försvarsmaktens långsiktiga materielbehov. Fö.
8. Kunskapsläget på kärnavfallsområdet 2018. Beslut under osäkerhet. M.
9. Ökad trygghet för studerande som blir sjuka. U.
10. Myndighetsgemensam indelning – samverkan på regional nivå. Volym 1. Myndighetsgemensam indelning – författningsändringar till följd av ny landstingsbeteckning. Volym 2. Fi.
11. Vårt gemensamma ansvar – för unga som varken arbetar eller studerar. U.
12. Uppdrag: Samverkan 2018. Många utmaningar återstår. A.
13. Finansiering av infrastruktur med skatt eller avgift? Fi.
14. Bidragsbrott och underrättelseskyldighet vid felaktiga utbetalningar från välfärdssystemen – en utvärdering. Fi.
15. Mindre aktörer i energilandskapet – genomgång av nuläget. M.
16. Vägen till självkörande fordon – introduktion. Del 1 + 2. N.
17. Med undervisningsskicklighet i centrum – ett ramverk för lärares och rektorers professionella utveckling. U.
18. Statens stöd till trossamfund i ett mångreligiöst Sverige. Ku.
19. Forska tillsammans – samverkan för lärande och förbättring. U.
20. Gräsrotsfinansiering. Fi.
21. Flexibel rehabilitering. A.
22. Ett ordnat mottagande – gemensamt ansvar för snabb etablering eller återvändande. A.
23. Konstnär – oavsett villkor? Ku.
24. Tid för utveckling. A.
25. Juridik som stöd för förvaltningens digitalisering. Fi.
26. Några frågor i skyddslagstiftningen. Fö.
27. Ekonomiska sanktioner mot terrorism. UD.
28. En nationell alarmeringstjänst – för snabba, säkra och effektiva hjälpinsatser. Ju.
29. Validering i högskolan – för tillgodoräknande och livslångt lärande. U.
30. Förenklat förfarande vid vissa beslut om hemlig avlyssning. Ju.
31. En lag om operativt militärt stöd mellan Sverige och Finland. Fö.
32. Ju förr desto bättre – vägar till en förebyggande socialtjänst. S.
33. Aggressionsbrottet och ändringar i Romstadgan. Ju.
34. Vägar till hållbara vattentjänster. M.
35. Ett gemensamt bostadsförsörjningsansvar. N.
36. Rätt att forska. Långsiktig reglering av forskningsdatabaser. U.
37. Att bryta ett våldsamt beteende – återfallsförebyggande insatser för män som utsätter närstående för våld. S.

38. Styra och leda med tillit. Forskning och praktik. Fi.
39. God och nära vård. En primärvårdsreform. S.
40. Vissa fredspliktsfrågor. A.
41. Statliga skolmyndigheter. – för elever och barn i en bättre skola. U.
42. Tryggad tillgång till kontanter. Fi.
43. Statliga servicekontor – mer service på fler platser. Fi.
44. Möjligt, tillåtet och tillgängligt – förslag till enklare och flexiblare upphandlingsregler och vissa regler om överprövningsmål. Fi.
45. Behandling av personuppgifter vid Myndigheten för arbetsmiljökunskap. A.
46. En utvecklad översiktsplanering. Del 1: Att underlätta efterföljande planering. Del 2: Kommunal reglering av upplåtelseformen. N.
47. Med tillit växer handlingsutrymmet. – tillitsbaserad styrning och ledning av välfärdssektorn. Fi.
48. En lärande tillsyn. Statlig granskning som bidrar till verksamhetsutveckling i vård, skola och omsorg. Fi.
49. F-skattesystemet – några särskilt utpekade frågor. Fi.
50. Ett oberoende public service för alla – nya möjligheter och ökat ansvar. Ku.
51. Resurseffektiv användning av byggmaterial. N.
52. Behandling av personuppgifter vid Myndigheten för vård- och omsorgsanalys. S.
53. Översyn av maskinell dos, extempore, prövningsläkemedel m.m. S.
54. En effektivare kommunal räddningstjänst. Ju.
55. Styrning och vårdkonsumtion ur ett jämlikhetsperspektiv. Kartläggning av socioekonomiska skillnader i vårdutnyttjande och utgångspunkter för bättre styrning. S.
56. Bättre kommunikation för fler investeringar. UD.
57. Barns och ungas läsning – ett ansvar för hela samhället. Ku.
58. Särskilda persontransporter – moderniserad lagstiftning för ökad samordning. N.
59. Statens gruvliga risker. M.
60. Tillträde till Rotterdamreglerna. Ju.
61. Rättssäkerhetsgarantier och hemliga tvångsmedel. Ju.
62. Kamerabevakning i brottsbekämpningen – ett enklare förfarande. Ju.
63. Behandlingen av personuppgifter vid Försvarsmakten och Försvarets radioanstalt. Fö.

Statens offentliga utredningar 2018

Systematisk förteckning

Kulturdepartementet

Statens stöd till trossamfund i ett mångreligiöst Sverige. [18]

Konstnär – oavsett villkor? [23]

Ett oberoende public service för alla – nya möjligheter och ökat ansvar. [50]

Barns och ungas läsning – ett ansvar för hela samhället. [57]

Miljö- och energidepartementet

Kunskapsläget på kärnavfallsområdet 2018. Beslut under osäkerhet. [8]

Mindre aktörer i energilandskapet – genomgång av nuläget. [15]

Vägar till hållbara vattentjänster. [34]

Statens gruvliga risker. [59]

Näringsdepartementet

Vägen till självkörande fordon – introduktion. Del 1 + 2. [16]

Ett gemensamt bostadsförsörjningsansvar. [35]

En utvecklad översiktsplanering. Del 1: Att underlätta efterföljande planering. Del 2: Kommunal reglering av upplåtelseformen. [46]

Resurseffektiv användning av byggmaterial. [51]

Särskilda persontransporter – moderniserad lagstiftning för ökad samordning. [58]

Socialdepartementet

Framtidens biobanker. [4]

Vissa processuella frågor på socialförsäkringsområdet. [5]

Ju förr desto bättre – vägar till en förebyggande socialtjänst. [32]

Att bryta ett våldsamt beteende – återfallsförebyggande insatser för män som utsätter närstående för våld. [37]

God och nära vård. En primärvårdsreform. [39]

Behandling av personuppgifter vid Myndigheten för vård- och omsorgsanalys. [52]

Översyn av maskinell dos, extempore, prövningsläkemedel m.m. [53]

Styrning och vårdkonsumtion ur ett jämlikhetsperspektiv. Kartläggning av socioekonomiska skillnader i vårdutnyttjande och utgångspunkter för bättre styrning. [55]

Utbildningsdepartementet

En strategisk agenda för internationalisering. [3]

Ökad trygghet för studerande som blir sjuka. [9]

Vårt gemensamma ansvar – för unga som varken arbetar eller studerar. [11]

Med undervisningsskicklighet i centrum – ett ramverk för lärares och rektorers professionella utveckling. [17]

Forska tillsammans – samverkan för lärande och förbättring. [19]

Validering i högskolan – för tillgodoräknande och livslångt lärande. [29]

Rätt att forska. Långsiktig reglering av forskningsdatabaser. [36]

Statliga skolmyndigheter. – för elever och barn i en bättre skola. [41]

Utrikesdepartementet

Ekonomiska sanktioner mot terrorism. [27]

Bättre kommunikation för fler investeringar. [56]