Regeringens proposition 2020/21:224

Behandling av personuppgifter vid Försvarsmakten och Försvarets radioanstalt

Prop. 2020/21:224

Regeringen överlämnar denna proposition till riksdagen.

Stockholm den 9 september 2021

Stefan Löfven

Peter Hultqvist
(Försvarsdepartementet)

Propositionens huvudsakliga innehåll

I propositionen föreslås två nya lagar om behandling av personuppgifter vid Försvarsmakten respektive Försvarets radioanstalt. De nya lagarna föreslås ersätta lagen om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst och lagen om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet, som enligt förslaget upphävs. Det föreslås även följdändringar i vissa lagar. Vidare föreslås ändringar i lagen om signalspaning i försvarsunderrättelseverksamhet som bland annat rör Försvarets radioanstalts internationella samarbete.

Genom de nya lagarna skyddas fysiska personers grundläggande rättigheter och friheter samtidigt som det säkerställs att Försvarsmakten och Försvarets radioanstalt kan behandla och utbyta personuppgifter med andra aktörer på ett ändamålsenligt sätt. De nya lagarna ska tillämpas i stället för EU:s dataskyddsförordning och dataskyddslagen.

De nya lagarna och övriga lagändringar föreslås träda i kraft den 1 januari 2022.

Innehållsförteckning

1 Förslag till riksdagsbeslut 7

2 Lagtext 8
- 2.1 Förslag till lag om behandling av personuppgifter vid Försvarsmakten 8
- 2.2 Förslag till lag om behandling av personuppgifter vid Försvarets radioanstalt 21
- 2.3 Förslag till lag om ändring i lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet 33
- 2.4 Förslag till lag om ändring i lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning 36
- 2.5 Förslag till lag om ändring i brottsdatalagen (2018:1177) 37

3 Ärendet och dess beredning 38

4 Försvarsmakten och Försvarets radioanstalt 39
- 4.1 Försvarsmakten 39
  - 4.1.1 Försvarsmaktens uppgifter 39
  - 4.1.2 Försvarsmaktens militära säkerhetstjänst 40
  - 4.1.3 Internationellt samarbete 41
- 4.2 Försvarets radioanstalt 42
  - 4.2.1 Försvarets radioanstalts uppgifter 42
  - 4.2.2 Försvarets radioanstalts informationssäkerhetsverksamhet 43
- 4.3 Försvarsmaktens och Försvarets radioanstalts försvarsunderrättelseverksamhet 43
- 4.4 Försvarets radioanstalts signalspaning i försvarsunderrättelse- och utvecklingsverksamhet 45
  - 4.4.1 Gällande reglering 45
  - 4.4.2 Internationellt samarbete 46
- 4.5 Försvarsmaktens och Försvarets radioanstalts behandling av personuppgifter 47
  - 4.5.1 Gällande reglering 47
  - 4.5.2 Exempel på annan reglering som gäller för Försvarsmakten 48
  - 4.5.3 Exempel på annan reglering som gäller för Försvarets radioanstalt 48

5 Det grundläggande skyddet för personuppgifter 49
- 5.1 Regeringsformen och Europakonventionen 49
- 5.2 Europarådets dataskyddskonvention 50
- 5.3 Europeiska unionen 51
  - 5.3.1 EU-stadgan 51
  - 5.3.2 1995 års dataskyddsdirektiv 52
  - 5.3.3 EU:s dataskyddsförordning 52
  - 5.3.4 2016 års dataskyddsdirektiv 53

6 Allmänna utgångspunkter för en ny reglering 54
- 6.1 Två nya lagar införs 54

6.2 Förhållandet till EU:s dataskyddsförordning ... 55
6.3 Syftet med de nya lagarna ... 57
6.4 De nya lagarnas tillämpningsområden ... 58
6.4.1 Tillämpningsområdet för lagen om behandling av personuppgifter vid Försvarsmakten ... 58
6.4.2 Tillämpningsområdet för lagen om behandling av personuppgifter vid Försvarets radioanstalt ... 60
6.5 Vissa ord och uttryck i lagarna ska definieras ... 61

7 Ändamål för behandlingen av personuppgifter ... 65
7.1 Behandling får bara ske för särskilda, uttryckligt angivna och berättigade ändamål ... 65
7.2 Försvarsmakten ... 67
7.2.1 Försvar och säkerhet ... 67
7.2.2 Försvarsmaktens försvarsunderrättelseverksamhet ... 70
7.2.3 Militär säkerhetstjänst ... 72
7.2.4 Signalkontrollverksamhet ... 75
7.2.5 Ärendehandläggning och liknande uppgifter ... 76
7.3 Försvarets radioanstalt ... 77
7.3.1 Försvarets radioanstalts försvarsunderrättelseverksamhet ... 77
7.3.2 Utvecklingsverksamhet ... 80
7.3.3 Informationssäkerhetsverksamhet ... 82
7.4 Behandling av allmänt tillgänglig information ... 84
7.5 Behandling för vetenskapliga, statistiska eller historiska ändamål ... 86
7.6 Behandling av uppgifter om lagöverträdelser ... 87

8 Behandlingen av personuppgifter ... 88
8.1 Personuppgifter ska behandlas enligt vissa villkor ... 88
8.1.1 Personuppgifter ska behandlas författningsenligt och på ett korrekt sätt ... 88
8.1.2 Personuppgifter ska vara riktiga, adekvata och relevanta ... 88
8.2 Behandling av känsliga personuppgifter ... 90
8.3 Behandling av personnummer och samordningsnummer ... 93
8.4 Behandling av offentliggjorda personuppgifter ... 94
8.5 Behandling av personuppgifter i vissa fall ... 94
8.6 Längsta tid som personuppgifter får behandlas ... 97

9 Gemensamt tillgängliga personuppgifter ... 98

10 Informationsutbyte ... 101
10.1 Olika former av elektroniskt utlämnande ... 101
10.2 Elektronisk informationsöverföring på annat sätt än direktåtkomst ... 102
10.3 Direktåtkomst ... 103
10.3.1 Direktåtkomst för svenska myndigheter ... 103

10.3.2 Direktåtkomst för utländska myndigheter och internationella organisationer 108
10.4 Sekretessbrytande bestämmelser 111
10.4.1 Varför behövs sekretessbrytande bestämmelser? 111
10.4.2 Sekretessbrytande bestämmelser gentemot svenska myndigheter 113
10.5 Överföring av personuppgifter till andra länder och internationella organisationer 116

11 Personuppgiftsansvar 121
11.1 Vem är personuppgiftsansvarig? 121
11.2 Ingen reglering av gemensamt personuppgiftsansvar 121
11.3 Skyldigheter som personuppgiftsansvarig 123
11.3.1 Författningsenlig behandling genom lämpliga tekniska och organisatoriska åtgärder 123
11.3.2 Säkerheten för personuppgifter 124
11.3.3 Inget krav på en särskild konsekvensbedömning 125
11.3.4 Ingen skyldighet att anmäla personuppgiftsincidenter 125
11.4 Dataskyddsombud 126
11.5 Personuppgiftsbiträden 130
11.5.1 Definition av personuppgiftsbiträde 130
11.5.2 Anlitande av personuppgiftsbiträden 131
11.5.3 Behandling enligt den personuppgiftsansvariges instruktioner 132
11.5.4 Övriga skyldigheter för personuppgiftsbiträden 132

12 Enskildas rättigheter 133
12.1 Rätten till information 133
12.1.1 Information som ska göras allmänt tillgänglig 133
12.1.2 Enskildas rätt till personrelaterad information 134
12.2 Rätten till information får begränsas 136
12.3 Rättelse, radering och begränsning av behandlingen 138

13 Tillsyn 142
13.1 Nuvarande ordning 142
13.2 Former för tillsyn till skydd för den personliga integriteten 144
13.3 Tillsynsmyndighetens befogenheter 145
13.3.1 Undersökningsbefogenheter 145
13.3.2 Förebyggande befogenheter 146
13.3.3 Korrigerande befogenheter 147

14 Sanktioner, skadestånd och rättsmedel 149
14.1 Ingen straffbestämmelse i de nya lagarna 149
14.2 Ingen möjlighet att ta ut sanktionsavgift 150
14.3 Skadestånd 151

14.3.1 Det allmännas skadeståndsansvar ... 151
14.3.2 Skadeståndsansvar för den personuppgiftsansvarige ... 152
14.4 Överklagande ... 154
14.4.1 Överklagande av Försvarsmaktens och Försvarets radioanstalts beslut ... 154
14.4.2 Överklagande av tillsynsmyndighetens beslut ... 155
15 Ändringar i lagen om signalspaning i försvarsunderrättelseverksamhet ... 156
15.1 Signalspaning vid internationellt samarbete ... 156
15.2 Regeringen ska inrikta signalspaningen vid internationellt samarbete ... 158
15.3 Förstöringsskyldigheten preciseras ... 159
16 Följdändringar i andra författningar ... 162
17 Ikraftträdande- och övergångsbestämmelser ... 163
18 Konsekvenser ... 165
19 Författningskommentar ... 167
19.1 Förslaget till lag om behandling av personuppgifter vid Försvarsmakten ... 167
19.2 Förslaget till lag om behandling av personuppgifter vid Försvarets radioanstalt ... 206
19.3 Förslaget till lag om ändring i lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet ... 242
19.4 Förslaget till lag om ändring i lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning ... 245
19.5 Förslaget till lag om ändring i brottsdatalagen (2018:1177) ... 245
Bilaga 1 Sammanfattning av betänkandet Personuppgiftsbehandlingen vid Försvarsmakten och Försvarets radioanstalt (SOU 2018:63) ... 247
Bilaga 2 Lagförslagen i betänkandet SOU 2018:63 ... 252
Bilaga 3 Förteckning över remissinstanserna (betänkandet SOU 2018:63) ... 279
Bilaga 4 Sammanfattning av betänkandet Försvarets radioanstalts internationella samarbete – en översyn av regelverket (SOU 2020:68) ... 280
Bilaga 5 Lagförslagen i betänkandet SOU 2020:68 ... 283
Bilaga 6 Förteckning över remissinstanserna (betänkandet SOU 2020:68) ... 287
Bilaga 7 Lagrådsremissens lagförslag ... 288
Bilaga 8 Lagrådets yttrande ... 317

Prop. 2020/21:224 Utdrag ur protokoll vid regeringssammanträde den 9 september 2021 326

1 Förslag till riksdagsbeslut

Regeringens förslag:

1. Riksdagen antar regeringens förslag till lag om behandling av personuppgifter vid Försvarsmakten.
2. Riksdagen antar regeringens förslag till lag om behandling av personuppgifter vid Försvarets radioanstalt.
3. Riksdagen antar regeringens förslag till lag om ändring i lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet.
4. Riksdagen antar regeringens förslag till lag om ändring i lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.
5. Riksdagen antar regeringens förslag till lag om ändring i brottsdatalagen (2018:1177).

2 Lagtext

Regeringen har följande förslag till lagtext.

2.1 Förslag till lag 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 i verksamhet som rör Sveriges försvar och säkerhet samt internationellt försvars- och säkerhetssamarbete.

3 § Lagen gäller vid sådan behandling av personuppgifter som är helt eller delvis automatiserad. Den gäller också personuppgifter som ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

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

Ord och uttryck i lagen

5 § I denna lag används följande ord och uttryck.

Ord och uttryck	*Betydelse*
Behandling av personuppgifter	En åtgärd eller en kombination av åtgärder som vidtas i fråga om personuppgifter eller uppsättningar av personuppgifter, oavsett om det görs automatiserat eller inte, t.ex. insamling, registrering, organise-

	ring, 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 identifiering av personen i fråga.
Dataskyddsombud	En fysisk person som utses av den personuppgiftsansvarige för att självständigt kontrollera att personuppgifter behandlas författningsenligt och på ett korrekt sätt.
Genetiska uppgifter	Personuppgifter som rör en persons nedärvda eller förvärvade genetiska kännetecken och som framför allt härrör från analys av ett spår av eller ett biologiskt prov från personen i fråga.
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 behandlar personuppgifter för den personuppgiftsansvariges räkning.
Registrerad	Den fysiska person som personuppgiften gäller.

Tredje part	Någon annan än – den registrerade, – den 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.

Personuppgiftsansvar

6 § Försvarsmakten är personuppgiftsansvarig för all behandling av personuppgifter som myndigheten utför, som utförs under myndighetens ledning eller på dess vägnar.

2 kap. Behandling av personuppgifter

Grundläggande krav på behandlingen

Krav på ändamål

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

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

Försvar och säkerhet

2 § 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, kollektivavtal eller annat avtal, eller ett särskilt beslut där regeringen har gett myndigheten i uppdrag att utföra uppgiften.

För Försvarsmaktens behandling av personuppgifter i myndighetens försvarsunderrättelseverksamhet och militära säkerhetstjänst gäller i stället 3–8 §§.

Försvarsunderrättelseverksamhet

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

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

Första stycket gäller endast om inte något annat följer av denna lag eller en förordning som regeringen har meddelat i anslutning till lagen.

Militär säkerhetstjänst

5 § 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.

6 § Personuppgifter får behandlas för de ändamål som anges i 5 § endast om

1. personuppgifterna 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 enligt motsvarande äldre föreskrifter,
2. personuppgifterna är nödvändiga för att kartlägga underrättelseverksamhet som riktas mot Försvarsmakten och dess säkerhetsintressen,
3. personuppgifterna är nödvändiga för att kartlägga annan säkerhetshotande verksamhet än som avses i 1 och som innefattar brott eller åsidosättande av skyldigheter i anställning hos Försvarsmakten, och det finns särskilda skäl till att uppgiften ska behandlas,
4. personuppgifterna är nödvändiga för att bedöma om en person som har lämnat uppgifter om säkerhetshotande verksamhet är trovärdig, eller
5. personuppgifterna är nödvändiga för att genomföra säkerhetsprövning enligt säkerhetsskyddslagen (2018:585) eller för att utföra en uppgift som rör säkerhetsskydd.

7 § Personuppgifter som behandlas enligt 6 § ska förses med upplysning om på vilken av de angivna grunderna uppgiften behandlas.

Om behandlingen av en personuppgift motiveras av något annat än ett antagande om att en person 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 en 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 ett sådant antagande inte finns.

Personuppgifter som behandlas enligt 6 § 1, 2 eller 3 ska i förekommande fall förses med en upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak.

8 § Trots 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 på 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 6 § 1, 2 eller 3 tillämpas.

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

Övriga ändamål

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

10 § Försvarsmakten får behandla personuppgifter som utgör allmänt tillgänglig information om det är nödvändigt för den verksamhet som anges i 2, 3 och 5 §§.

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

12 § Försvarsmakten får behandla personuppgifter om lagöverträdelser om det är nödvändigt för myndighetens verksamhet.

Författningsenlig och korrekt behandling

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

Personuppgifternas kvalitet

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

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 personuppgifter behandlas får de dock kompletteras med sådana uppgifter som avses i första stycket, om det är absolut nödvändigt med hänsyn till ändamålen med behandlingen.

16 § Biometriska uppgifter får behandlas om det är absolut nödvändigt med hänsyn till ändamålen med 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 med hänsyn till ändamålen med behandlingen. Detsamma gäller biometriska uppgifter.

Personnummer och samordningsnummer

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

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

Om den registrerade har lämnat sitt samtycke eller offentliggjort personuppgifterna

19 § Trots 15, 16 och 18 §§ får andra personuppgifter än genetiska uppgifter behandlas, om den registrerade har lämnat sitt uttryckliga samtycke eller på ett tydligt sätt har offentliggjort uppgifterna.

Behandling av personuppgifter i vissa fall

20 § Hantering av information som innebär behandling av personuppgifter ska inte anses oförenlig med bestämmelserna i 1–3, 5, 6, 8, 10, 12–16 och 18 §§ i det skede av behandlingen då det inte har kunnat fastställas vilka personuppgifter som informationen innehåller.

Längsta tid som personuppgifter får behandlas

21 § Personuppgifter får inte behandlas under längre tid än vad som behövs med hänsyn till ändamålen med behandlingen.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om att personuppgifter får behandlas under endast viss tid eller fortsätta behandlas för arkivändamål av allmänt intresse eller för vetenskapliga, statistiska eller historiska ändamål.

Regeringen eller den myndighet som regeringen bestämmer får också besluta om sådan behandling i ett enskilt fall.

Överföring av personuppgifter till en mottagare utomlands

22 § Personuppgifter som behandlas med stöd av denna lag får föras över till ett annat land eller en internationell organisation 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 med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om att överföring får ske även i andra fall om det är nödvändigt för verksamheten vid Försvarsmakten.

Regeringen får också besluta om sådan överföring i ett enskilt fall.

Utlämnande av personuppgifter

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

Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om begränsning av möjligheten att lämna ut personuppgifter elektroniskt på annat sätt än genom direktåtkomst.

3 kap. Gemensamt tillgängliga personuppgifter

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. Med att göra personuppgifter gemensamt tillgängliga avses inte att endast ett fåtal personer får tillgång till uppgifterna.

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

Regeringen eller den myndighet som regeringen bestämmer får också besluta om uppgiftssamlingar i ett enskilt fall.

Direktåtkomst

2 § Totalförsvarets plikt- och prövningsverk får medges direktåtkomst till personuppgifter som rör Försvarsmaktens personalförsörjning och krigsorganisation och som har gjorts gemensamt tillgängliga inom Försvarsmakten.

Totalförsvarets plikt- och prövningsverk har rätt att vid direktåtkomst ta del av de personuppgifter som omfattas av åtkomsten.

3 § Säkerhetspolisen och Försvarets radioanstalt får medges direktåtkomst till personuppgifter som utgör bearbetningsunderlag och analysresultat inom försvarsunderrättelseverksamheten och som finns i uppgiftssamlingar.

Säkerhetspolisen och Försvarets radioanstalt har rätt att vid direktåtkomst ta del av de personuppgifter som omfattas av åtkomsten.

4 § 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 med stöd av 2 kap. 3 § och som finns i uppgiftssamlingar.

Första stycket gäller enbart i den utsträckning som sådan direktåtkomst följer av lag eller förordning eller om regeringen har beslutat om den i ett enskilt fall.

5 § 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 § och som finns i uppgiftssamlingar.

Första stycket gäller enbart i den utsträckning som sådan direktåtkomst följer av lag eller förordning eller om regeringen har beslutat om den i ett enskilt fall.

Direktåtkomst i andra fall

6 § Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om direktåtkomst till gemensamt tillgängliga uppgifter eller uppgiftssamlingar i andra fall än de som anges i 2–5 §§.

Regeringen får också besluta om detta i ett enskilt fall.

Omfattningen av direktåtkomsten

7 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om omfattningen av direktåtkomsten och om behörighet och säkerhet vid sådan åtkomst.

Regeringen får också besluta om detta i ett enskilt fall.

4 kap. Skyldigheter 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 att de registrerades rättigheter skyddas.

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

Säkerheten för personuppgifter

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

Dataskyddsombud

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

5 § Ett dataskyddsombud 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. vara kontaktpunkt för enskilda i frågor som rör Försvarsmaktens behandling av personuppgifter, och

4. vid behov söka vägledning av tillsynsmyndigheten.

Personuppgiftsbiträden

6 § 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 registrerades rättigheter.

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

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

9 § 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.

10 § Försvarsmaktens skyldigheter enligt 2 och 3 §§ gäller även för personuppgiftsbiträden som Försvarsmakten anlitar.

5 kap. Enskildas rättigheter

Rätten till information

Allmän information

1 § Försvarsmakten ska göra följande information allmänt tillgänglig:

1. myndighetens identitet och kontaktuppgifter,
2. uppgifter om dataskyddsombudet,
3. kategorier av ändamål för behandlingen av personuppgifter,
4. rätten enligt 3 § att begära att få information om behandlingen av personuppgifter och att få del av dem, och
5. rätten att begära rättelse, radering eller begränsning av behandlingen enligt 6 §.

Information som ska lämnas om personuppgifterna samlas in från den som uppgifterna avser

2 § Om personuppgifter samlas in från den som uppgifterna avser ska Försvarsmakten, när myndigheten får personuppgifterna, på eget initiativ lämna följande information till den registrerade:

1. uppgift om att det är Försvarsmakten som är personuppgiftsansvarig för behandlingen,
2. uppgift om ändamålen med behandlingen, och

3. all övrig information som behövs för att den registrerade ska kunna ta till vara sina rättigheter i samband med behandlingen, såsom information om uppgifternas mottagare, om skyldighet att lämna uppgifter och om 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 huruvida personuppgifter som rör honom eller henne behandlas. Om sådana uppgifter behandlas ska sökanden få del av dem och få följande skriftliga information:

1. vilka personuppgifter om den sökande som behandlas,
2. varifrån personuppgifterna kommer,
3. ändamålen med behandlingen,
4. mottagare eller kategorier av mottagare av personuppgifterna, även i annat land eller internationella organisationer,
5. hur länge personuppgifterna får behandlas eller, om det inte är möjligt att ange, kriterierna för att fastställa det, och
6. rätten att begära rättelse, radering eller begränsning av behandlingen enligt 6 §.

Ett utlämnande av personuppgifter enligt första stycket behöver inte omfatta sådana 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 om information enligt första stycket ska göras skriftligen hos Försvarsmakten och vara undertecknad av den sökande själv. Informationen 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 enligt 2 och 3 §§ gäller inte i den utsträckning sekretess hindrar att uppgifterna lämnas ut.

Om det gäller sekretess är Försvarsmakten inte skyldig att redovisa skälen för ett beslut enligt första stycket eller ett beslut i fråga om rättelse, radering eller begränsning av behandlingen enligt 6 §.

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

Informationsskyldigheten gäller dock om uppgifterna

1. har lämnats ut till tredje part, med undantag för en myndighet som med stöd av författning utövar tillsyn, kontroll eller revision,
2. behandlas enbart för statistiska ändamål eller arkivändamål av allmänt intresse, eller
3. har behandlats under längre tid än ett år i löpande text som inte har fått sin slutliga utformning.

Rätten till rättelse, radering och begränsning av behandlingen

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

Om uppgifterna har lämnats ut till tredje part ska denne underrättas om en åtgärd enligt första stycket, om den registrerade begär det eller om en mera betydande skada eller olägenhet för den registrerade 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 §§ och information och uppgifter enligt 3 § ska lämnas utan avgift.

6 kap. Tillsyn

Tillsyn över personuppgiftsbehandlingen

1 § Den myndighet som regeringen bestämmer utövar tillsyn över Försvarsmaktens behandling av personuppgifter enligt denna lag, enligt föreskrifter som har meddelats i anslutning till lagen och enligt beslut med stöd av lagen.

Tillsynsmyndigheten ska, när det är motiverat, ge råd och stöd till Försvarsmakten och personuppgiftsbiträden i frågor som gäller deras skyldigheter enligt lag eller annan författning.

Tillsynsmyndighetens befogenheter

Undersökningsbefogenheter

2 § Tillsynsmyndigheten har rätt att av Försvarsmakten eller av 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. den hjälp 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 motverka den risken.

Tillsynsmyndigheten får besluta om en skriftlig varning, om en planerad behandling av personuppgifter riskerar att strida mot lag eller annan

författning. Detsamma gäller om en pågående behandling riskerar att strida mot 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 på annat sätt 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 för att fullgöra andra skyldigheter, eller
2. besluta att förelägga Försvarsmakten eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsenlig eller för att fullgöra andra skyldigheter.

Av ett beslut om föreläggande ska det framgå när föreläggandet senast ska ha följts och, om det är lämpligt, vilka åtgärder som ska vidtas.

7 kap. Skadestånd och överklagande

Skadestånd

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

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

Överklagande

Överklagande av Försvarsmaktens beslut

2 § Försvarsmaktens beslut enligt 5 kap. 2 och 3 §§ att inte lämna information och beslut enligt 5 kap. 6 § i fråga om rättelse, radering, begränsning av behandlingen eller underrättelse till tredje part, får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Överklagande av tillsynsmyndighetens beslut

3 § Tillsynsmyndighetens beslut om föreläggande enligt 6 kap. 4 § första stycket 2 får överklagas till allmän förvaltningsdomstol. När ett beslut överklagas är tillsynsmyndigheten motpart i domstolen.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Överklagandeförbud

4 § Andra beslut enligt denna lag än de som anges i 2 och 3 §§ får inte överklagas.

---

1. Denna lag träder i kraft den 1 januari 2022.

2. Genom lagen upphävs lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst.

3. Äldre föreskrifter gäller fortfarande för överklagande av beslut som har meddelats före ikraftträdandet.

2.2 Förslag till lag 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. Den gäller också personuppgifter som ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

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

Ord och uttryck i lagen

5 § I denna lag används följande ord och uttryck.

Ord och uttryck	*Betydelse*
Behandling av personuppgifter	En åtgärd eller en 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, samman-

	föring, 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 identifiering av personen i fråga.
Dataskyddsombud	En fysisk person som utses av den personuppgiftsansvarige för att självständigt kontrollera att personuppgifter behandlas författningsenligt och på ett korrekt sätt.
Genetiska uppgifter	Personuppgifter som rör en persons nedärvda eller förvärvade genetiska kännetecken och som framför allt härrör från analys av ett spår av eller ett biologiskt prov från personen i fråga.
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 behandlar personuppgifter för den personuppgiftsansvariges räkning.
Registrerad	Den fysiska person som personuppgiften gäller.
Tredje part	Någon annan än – den registrerade, – den 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.

Personuppgiftsansvar

6 § Försvarets radioanstalt är personuppgiftsansvarig för all behandling av personuppgifter som myndigheten utför, som utförs under myndighetens ledning eller på dess vägnar.

2 kap. Behandling av personuppgifter

Grundläggande krav på behandlingen

Krav på ändamål

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

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

Försvarsunderrättelseverksamhet

2 § 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.

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

Första stycket gäller endast om inte något annat följer av denna lag eller en förordning som regeringen har meddelat i anslutning till lagen.

4 § Personuppgifter som behandlas med stöd av 2 och 3 §§ 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 om försvarsunderrättelseverksamhet och lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet,
3. i utvecklingsverksamheten för de ändamål som anges i 5 §,
4. i informationssäkerhetsverksamheten för de ändamål som anges i 7 §, eller

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

Utvecklingsverksamhet

5 § 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.

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

1. med anledning av samverkan med annan i fråga om 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 2 och 3 §§,
4. i informationssäkerhetsverksamheten för de ändamål som anges i 7 §, eller
5. för att biträda andra myndigheter i den utsträckning det följer av lag eller förordning eller om regeringen har beslutat om det i ett enskilt fall.

Informationssäkerhetsverksamhet

7 § 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 beslut av regeringen i ett enskilt fall.

8 § Personuppgifter som behandlas med stöd av 7 § 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 har beslutat om det i ett enskilt fall,
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 5 §.

Övriga ändamål

9 § Försvarets radioanstalt får behandla personuppgifter som utgör allmänt tillgänglig information om det är nödvändigt för den verksamhet som anges i 2, 5 och 7 §§.

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

Författningsenlig och korrekt behandling

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

Personuppgifternas kvalitet

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

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

13 § 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 personuppgifter behandlas får de dock kompletteras med sådana uppgifter som avses i första stycket, om det är absolut nödvändigt med hänsyn till ändamålen med behandlingen.

14 § Biometriska uppgifter får behandlas om det är absolut nödvändigt med hänsyn till ändamålen med behandlingen.

Genetiska uppgifter får inte behandlas.

15 § 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 med hänsyn till ändamålen med behandlingen. Detsamma gäller biometriska uppgifter.

Personnummer och samordningsnummer

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

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

Om den registrerade har offentliggjort personuppgifterna

17 § Trots 13, 14 och 16 §§ får andra personuppgifter än genetiska uppgifter behandlas, om den registrerade på ett tydligt sätt har offentliggjort uppgifterna.

Behandling av personuppgifter i vissa fall

18 § Hantering av information som innebär behandling av personuppgifter ska inte anses oförenlig med bestämmelserna i 1, 2, 5, 7, 9, 11–14 och 16 §§ i det skede av behandlingen då det inte har kunnat fastställas vilka personuppgifter som informationen innehåller.

Längsta tid som personuppgifter får behandlas

19 § Personuppgifter får inte behandlas under längre tid än vad som behövs med hänsyn till ändamålen med behandlingen.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om att personuppgifter får behandlas under endast viss tid eller fortsätta behandlas för arkivändamål av allmänt intresse eller för vetenskapliga, statistiska eller historiska ändamål.

Regeringen eller den myndighet som regeringen bestämmer får också besluta om sådan behandling i ett enskilt fall.

Överföring av personuppgifter till en mottagare utomlands

20 § Personuppgifter som behandlas med stöd av denna lag får föras över till ett annat land eller en internationell organisation endast om det är nödvändigt för att Försvarets radioanstalt ska kunna fullgöra sina uppgifter inom ramen för det internationella försvarsunderrättelse- och säkerhetssamarbetet och

1. överföringen riktas till en utländsk underrättelse- eller säkerhetstjänst, eller ett underrättelse- eller säkerhetsorgan i en internationell organisation,
2. sekretess inte hindrar en överföring, och
3. mottagaren garanterar tillräckligt skydd för personuppgifterna.

Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om att överföring får ske även i andra fall än som anges i första stycket 1.

Regeringen får också besluta om sådan överföring i ett enskilt fall.

Utlämnande av personuppgifter

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

3 kap. Gemensamt tillgängliga personuppgifter

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. Med att göra personuppgifter gemensamt tillgängliga avses inte att endast ett fåtal personer får tillgång till uppgifterna.

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

Regeringen eller den myndighet som regeringen bestämmer får också besluta om uppgiftssamlingar i ett enskilt fall.

Direktåtkomst

Försvarsunderrättelseverksamhet

2 § Säkerhetspolisen och Försvarsmakten får medges direktåtkomst till personuppgifter som utgör analysresultat inom försvarsunderrättelseverksamheten och som finns i uppgiftssamlingar.

Säkerhetspolisen och Försvarsmakten har rätt att vid direktåtkomst ta del av de personuppgifter som omfattas av åtkomsten.

3 § Om det behövs för samarbetet mot terrorism eller för annat internationellt säkerhetssamarbete, får en utländsk underrättelse- eller säkerhetstjänst medges direktåtkomst till personuppgifter som behandlas med stöd av 2 kap. 2 § och som finns i uppgiftssamlingar.

Första stycket gäller enbart i den utsträckning som sådan direktåtkomst följer av lag eller förordning eller om regeringen har beslutat om den i ett enskilt fall.

Informationssäkerhetsverksamhet

4 § Om det behövs för samarbetet mot it-relaterade hot mot samhällsviktiga system, får en utländsk organisation inom informationssäkerhetsområdet medges direktåtkomst till personuppgifter som behandlas med stöd av 2 kap. 7 § och som finns i uppgiftssamlingar.

Första stycket gäller enbart i den utsträckning som sådan direktåtkomst följer av lag eller förordning eller om regeringen har beslutat om den i ett enskilt fall.

Direktåtkomst i andra fall

5 § Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om direktåtkomst till uppgiftssamlingar i andra fall än de som anges i 2–4 §§.

Regeringen får också besluta om detta i ett enskilt fall.

Omfattningen av direktåtkomsten

6 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om omfattningen av direktåtkomsten och om behörighet och säkerhet vid sådan åtkomst.

Regeringen får också besluta om detta i ett enskilt fall.

4 kap. Skyldigheter 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 att de registrerades rättigheter skyddas.

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

Säkerheten för personuppgifter

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

Dataskyddsombud

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

5 § Ett dataskyddsombud 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. vara kontaktpunkt för enskilda i frågor som rör Försvarets radioanstalts behandling av personuppgifter, och
4. vid behov söka vägledning av tillsynsmyndigheten.

Personuppgiftsbiträden

6 § 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 registrerades rättigheter.

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

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

9 § 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.

10 § Försvarets radioanstalts skyldigheter enligt 2 och 3 §§ gäller även för personuppgiftsbiträden som Försvarets radioanstalt anlitar.

5 kap. Enskildas rättigheter

Rätten till information

Allmän information

1 § Försvarets radioanstalt ska göra följande information allmänt tillgänglig:

1. myndighetens identitet och kontaktuppgifter,
2. uppgifter om dataskyddsombudet,
3. kategorier av ändamålen med behandlingen av personuppgifter,
4. rätten enligt 2 § att begära att få information om behandlingen av personuppgifter och att få del av dem, och
5. rätten att begära rättelse, radering eller begränsning av behandlingen enligt 5 §.

Information som ska lämnas efter begäran

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

1. vilka personuppgifter om den sökande som behandlas,
2. varifrån personuppgifterna kommer,
3. ändamålen med behandlingen,
4. mottagare eller kategorier av mottagare av personuppgifterna, även i annat land eller internationella organisationer,
5. hur länge personuppgifterna får behandlas eller, om det inte är möjligt att ange, kriterierna för att fastställa det, och
6. rätten att begära rättelse, radering eller begränsning av behandlingen enligt 5 §.

Ett utlämnande av personuppgifter enligt första stycket behöver inte omfatta sådana 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 om information enligt första stycket ska göras skriftligen hos Försvarets radioanstalt och vara undertecknad av den sökande själv. Informationen 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.

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

Om det gäller sekretess är Försvarets radioanstalt inte skyldig att redovisa skälen för ett beslut enligt första stycket eller ett beslut i fråga om rättelse, radering eller begränsning av behandlingen enligt 5 §.

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

Informationsskyldigheten gäller dock om uppgifterna

1. har lämnats ut till tredje part, med undantag för en myndighet som med stöd av författning utövar tillsyn, kontroll eller revision,
2. behandlas enbart för statistiska ändamål eller arkivändamål av allmänt intresse, eller
3. har behandlats under längre tid än ett år i löpande text som inte har fått sin slutliga utformning.

Rätten till rättelse, radering och begränsning av behandlingen

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

Om uppgifterna har lämnats ut till tredje part ska denne underrättas om en åtgärd enligt första stycket, om den registrerade begär det eller om en mera betydande skada eller olägenhet för den registrerade 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 § och information och uppgifter enligt 2 § ska lämnas utan avgift.

6 kap. Tillsyn

Tillsyn över personuppgiftsbehandlingen

1 § Den myndighet som regeringen bestämmer utövar tillsyn över Försvarets radioanstalts behandling av personuppgifter enligt denna lag, enligt föreskrifter som har meddelats i anslutning till lagen och enligt beslut med stöd av lagen.

Tillsynsmyndigheten ska, när det är motiverat, ge råd och stöd till Försvarets radioanstalt och personuppgiftsbiträden i frågor som gäller deras skyldigheter enligt lag eller annan författning.

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.

Tillsynsmyndighetens befogenheter

Undersökningsbefogenheter

3 § Tillsynsmyndigheten har rätt att av Försvarets radioanstalt eller av 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. den hjälp 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 motverka den risken.

Tillsynsmyndigheten får besluta om en skriftlig varning, om en planerad behandling av personuppgifter riskerar att strida mot lag eller annan författning. Detsamma gäller om en pågående behandling riskerar att strida mot 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 på annat sätt 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 för att fullgöra andra skyldigheter, eller
2. besluta att förelägga Försvarets radioanstalt eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsenlig eller för att fullgöra andra skyldigheter.

Av ett beslut om föreläggande ska det framgå när föreläggandet senast ska ha följts och, om det är lämpligt, vilka åtgärder som ska vidtas.

7 kap. Skadestånd och överklagande

Skadestånd

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

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

Överklagande

Överklagande av Försvarets radioanstalts beslut

2 § Försvarets radioanstalts beslut enligt 5 kap. 2 § att inte lämna information och beslut enligt 5 kap. 5 § i fråga om rättelse, radering, begränsning av behandlingen eller underrättelse till tredje part, får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Överklagande av tillsynsmyndighetens beslut

3 § Tillsynsmyndighetens beslut om föreläggande enligt 6 kap. 5 § första stycket 2 får överklagas till allmän förvaltningsdomstol. När ett beslut överklagas är tillsynsmyndigheten motpart i domstolen.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Överklagandeförbud

4 § Andra beslut enligt denna lag än de som anges i 2 och 3 §§ får inte överklagas.

---

1. Denna lag träder i kraft den 1 januari 2022.

2. Genom lagen upphävs lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet.

3. Äldre föreskrifter gäller fortfarande för överklagande av beslut som har meddelats före ikraftträdandet.

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

Härigenom föreskrivs att 1, 2 a, 4, 7 och 12 a §§ lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet ska ha följande lydelser.

Nuvarande lydelse	*Föreslagen lydelse*
1 §[1]	
I försvarsunderrättelseverksamhet enligt lagen (2000:130) om försvarsunderrättelseverksamhet får den myndighet som regeringen bestämmer (*signalspaningsmyndigheten*) inhämta signaler i elektronisk form vid signalspaning. Signalspaning i försvarsunderrättelseverksamhet får endast ske i de fall regeringen eller en myndighet som anges i 4 § närmare har bestämt inriktningen av signalspaningen.	
Signalspaning i försvarsunderrättelseverksamhet får ske endast i syfte att 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 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*	7. främmande underrättelseverksamhet mot svenska intressen,
8. främmande makts agerande eller avsikter av väsentlig betydelse för svensk utrikes-, säkerhets- eller försvarspolitik.	8. främmande makts agerande eller avsikter av väsentlig betydelse för svensk utrikes-, säkerhets- eller försvarspolitik, *eller*
	9. sådana företeelser som avses i 1–8, men som inte riktas mot Sverige eller rör svenska intressen, om det är nödvändigt för ett samarbete i underrättelsefrågor med andra länder och internationella organisationer som signalspaningsmyndigheten deltar i.

[1] Senaste lydelse 2009:967.

Om det är nödvändigt för försvarsunderrättelseverksamheten får signaler i elektronisk form inhämtas vid signalspaning även för att

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

2 a §[2]

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.	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. *Kravet på förstöring gäller även i fråga om upptagningar och uppteckningar som signalspaningsmyndigheten har fått från ett annat land eller en internationell organisation inom ramen för ett internationellt samarbete.*
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 *1. signaler som utväxlas autonomt mellan tekniska system i sådana fall där signalerna inte innehåller personuppgifter, eller* 2. *signaler som sänds från eller till utländsk militär personal,* utländska statsfartyg, statsluftfartyg eller militära fordon.

4 §[3]

I lagen (2000:130) om försvarsunderrättelseverksamhet finns bestämmelser om regeringens och myndigheters inriktning av sådan verksamhet. Inriktning av signalspaning får anges endast av regeringen, Regeringskansliet, Försvarsmakten, Säkerhetspolisen och Nationella operativa avdelningen i Polismyndigheten.

Regeringen bestämmer inriktningen av *den* verksamhet som bedrivs enligt 1 § tredje stycket.	Regeringen bestämmer inriktningen av *sådan* verksamhet som bedrivs enligt 1 § *andra stycket 9 och* tredje stycket.

En inriktning av signalspaningen får inte avse endast en viss fysisk person.

[2] Senaste lydelse 2009:967.
[3] Senaste lydelse 2014:691.

7 §[4]

En upptagning eller uppteckning av uppgifter som har inhämtats enligt denna lag ska omgående förstöras om innehållet	En upptagning eller uppteckning av uppgifter som har inhämtats enligt denna lag *eller som signalspaningsmyndigheten har fått från ett annat land eller en internationell organisation inom ramen för ett internationellt samarbete* ska omgående förstöras om innehållet

1. berör en viss fysisk person och har bedömts sakna betydelse för verksamhet som avses i 1 §,

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. 5 § tryckfrihetsförordningen eller 2 kap. 5 § 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.

12 a §[5]

I lagen *(2007:259)* om behandling av personuppgifter *i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet* finns ytterligare bestämmelser om behandlingen av inhämtade personuppgifter.	I lagen *(2021:000)* om behandling av personuppgifter *vid Försvarets radioanstalt* finns ytterligare bestämmelser om behandlingen av inhämtade personuppgifter.

Denna lag träder i kraft den 1 januari 2022.

[4] Senaste lydelse 2018:1918.
[5] Senaste lydelse 2009:967.

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

Härigenom föreskrivs i fråga om lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning[1]

dels att punkt 3 i ikraftträdande- och övergångsbestämmelserna ska upphöra att gälla,

dels att 1 kap. 3 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 kap.	
3 §[2]	
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 (2021:000) om behandling av personuppgifter vid Försvarsmakten*,
2. *lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet*, eller	2. *lagen (2021:000) om behandling av personuppgifter vid Försvarets radioanstalt*, eller
3. lagen (2019:1182) om Säkerhetspolisens behandling av personuppgifter.	

Denna lag träder i kraft den 1 januari 2022.

[1] Senaste lydelse av punkt 3 i ikraftträdande- och övergångsbestämmelserna 2020:152.
[2] Senaste lydelse 2019:1186.

2.5 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 i verksamhet *enligt lagen (2021:000) om behandling av personuppgifter vid Försvarsmakten*.

Denna lag träder i kraft den 1 januari 2022.

3 Ärendet och dess beredning

Med stöd av regeringens bemyndigande tillkallade chefen för Försvarsdepartementet den 27 april 2017 en särskild utredare med uppdrag att göra en översyn av den lagstiftning som gäller för personuppgiftsbehandling inom Försvarsmakten och Försvarets radioanstalt. Utredningen skulle bl.a. analysera huruvida nuvarande lagstiftning är ändamålsenlig för Försvarsmaktens och Försvarets radioanstalts verksamheter och om den är tillräcklig i fråga om skyddet för enskildas personliga integritet. Utredningen, som antog namnet Utredningen om behandlingen av personuppgifter vid Försvarsmakten och Försvarets radioanstalt, överlämnade den 9 augusti 2018 betänkandet Behandlingen av personuppgifter vid Försvarsmakten och Försvarets radioanstalt (SOU 2018:63).

Utredningens förslag behandlas i avsnitten 6–14 och 16–18. En sammanfattning av betänkandet finns i *bilaga 1*. Betänkandets lagförslag finns i *bilaga 2*.

Betänkandet har remissbehandlats. En förteckning över remissinstanserna finns i *bilaga 3*. Remissvaren finns tillgängliga på regeringens webbplats (www.regeringen.se) och i Försvarsdepartementet (Fö2018/00999).

Med stöd av regeringens bemyndigande tillkallade chefen för Försvarsdepartementet den 18 maj 2020 en särskild utredare med uppdrag att göra en översyn av regleringen av Försvarets radioanstalts internationella samarbete. Utredningen skulle bl.a. bedöma om regleringen av Försvarets radioanstalts internationella samarbete är effektiv och ändamålsenlig sett till myndighetens verksamhet och enskildas personliga integritet. Utredningen, som antog namnet Utredningen om regleringen av Försvarets radioanstalts internationella samarbete, överlämnade den 26 november 2020 betänkandet Försvarets radioanstalts internationella samarbete – en översyn av regelverket (SOU 2020:68).

Utredningens förslag behandlas i avsnitten 10.5 och 15, 17 och 18. En sammanfattning av betänkandet finns i *bilaga 4*. Betänkandets lagförslag finns i *bilaga 5*.

Betänkandet har remissbehandlats. En förteckning över remissinstanserna finns i *bilaga 6*. Remissvaren finns tillgängliga på regeringens webbplats (www.regeringen.se) och i Försvarsdepartementet (Fö2020/01191).

Lagrådet

Regeringen beslutade den 3 juni 2021 att inhämta Lagrådets yttrande över de lagförslag som finns i *bilaga 7*. Lagrådets yttrande finns i *bilaga 8*. Regeringen följer delvis Lagrådets förslag. Lagrådets synpunkter och förslag behandlas och bemöts i avsnitten 6.4.1, 7.2.1, 7.3.1, 7.3.3, 8.5, 9, 10.2, 11.1, 12.2 och i författningskommentaren.

I förhållande till lagrådsremissen har dessutom vissa språkliga och redaktionella ändringar gjorts.

4 Försvarsmakten och Försvarets radioanstalt

4.1 Försvarsmakten

4.1.1 Försvarsmaktens uppgifter

Försvarsmaktens grundläggande uppgifter framgår av förordningen (2007:1266) med instruktion 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. Försvarsmaktens huvuduppgift är att försvara Sverige mot ett väpnat angrepp (1 §). Försvarsmakten ska främja Sveriges säkerhet och hävda Sveriges territoriella integritet. Myndigheten ska ha förmåga att värna Sveriges suveräna rättigheter och svenska intressen samt att förebygga och hantera konflikter och krig såväl nationellt som internationellt. Försvarsmakten ska kunna utföra sina uppgifter självständigt eller i samverkan med andra myndigheter, stater eller organisationer. Försvarsmakten ska med myndighetens befintliga förmåga och resurser kunna lämna stöd till civil verksamhet (2 §).

Försvarsmakten ska organisera krigsförband och vidta de förberedelser i övrigt som behövs för att kunna lösa myndighetens huvuduppgift. Försvarsmakten ska planera för att kunna genomföra påskyndad krigsförbandsproduktion (2 a §). Försvarsmakten ska bedriva omvärldsbevakning och upptäcka och identifiera yttre hot mot Sverige och svenska intressen samt ta fram underlag för beslut om höjd beredskap. Försvarsmakten ska kunna ge och ta emot militärt stöd. Försvarsmakten ska med myndighetens tillgängliga resurser kunna påbörja operativ verksamhet omedelbart. Krigsorganisationen ska kunna mobiliseras. Försvarsmakten ska ha en aktuell försvarsplanering. Planeringen ska omfatta alla resurser som är nödvändiga för att genomföra Försvarsmaktens verksamhet. Försvarsmakten ska fortlöpande lämna upplysningar till berörda myndigheter om förhållanden i försvarsplaneringen som har betydelse för deras verksamhet (3 §). Försvarsmakten har även till uppgift att samordna försvarsplaneringen inom myndigheten med motsvarande planering inom övriga delar av totalförsvaret (7 §).

Försvarsmakten ska kunna delta i såväl kortvariga som långvariga internationella militära insatser och ta fram underlag för beslut om sådana insatser. Försvarsmakten ska kunna stödja och genomföra insatser för säkerhetssektorreform och bidra till uppbyggnaden av andra länders försvarsförmåga samt med myndighetens befintliga förmåga och resurser bidra till stöd för humanitär verksamhet. Försvarsmakten ska kunna genomföra räddnings-, evakuerings- och förstärkningsinsatser (3 a §).

Försvarsmakten ska vidare bedriva verksamhet enligt 1 § lagen (2000:130) om försvarsunderrättelseverksamhet (se avsnitt 4.3), 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 (3 b §).

Försvarsmakten ska även ansvara för att samla in, bearbeta och lämna Kustbevakningen sjölägesinformation, på uppdrag av Försvarets materielverk bedriva exportstödjande verksamhet inom försvarssektorn, medverka i statsceremonier och på begäran av polisen utföra helikoptertransporter enligt förordningen (2017:113) om Försvarsmaktens stöd till polisen med helikopterresurser, bedriva militär luftfart, kunna bedriva internationell militär test-, utbildnings-, och övningsverksamhet i Sverige och i Sverige och utomlands genomföra utbildning för svenska och utländska deltagare avseende internationell fredsfrämjande, säkerhetsfrämjande och konfliktförebyggande verksamhet (3 b, 3 c och 5 e §§).

För att upprätthålla och utveckla ett militärt försvar krävs utveckling av teknik och metodik. Försvarsmakten ska därför beställa forskning och utvecklingsarbete, samt bedriva egna studier och försök, för inriktning och utveckling av det militära försvaret (5 f §).

Försvarsmakten ansvarar för tillsynen över vissa myndigheters säkerhetsskydd enligt säkerhetsskyddslagen (2018:585). Tillsynen avser myndigheter som hör till Försvarsdepartementet samt Försvarshögskolan och Fortifikationsverket (7 kap. 1 § 1 säkerhetsskyddsförordningen [2018:658]).

4.1.2 Försvarsmaktens militära säkerhetstjänst

Försvarsmakten ska enligt sin instruktion leda och bedriva militär säkerhetstjänst. I säkerhetsskyddslagen finns bestämmelser om säkerhetsskydd. Med säkerhetsskydd avses enligt 1 kap. 2 § första stycket säkerhetsskyddslagen skydd av säkerhetskänslig verksamhet mot spionerі, sabotage, terroristbrott och andra brott som kan hota verksamheten samt skydd i andra fall av säkerhetsskyddsklassificerade uppgifter.

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 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.

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 (Personuppgiftsbehandling hos Försvarsmakten och Försvarets radioanstalt, prop. 2006/07:46 s. 25).

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.

Försvarsmakten bedriver även underrättelsetjänst för att kunna lösa militära uppgifter som inte utgör försvarsunderrättelseverksamhet eller militär säkerhetstjänst. Denna underrättelseverksamhet syftar främst till att skapa en lägesbild och ge beslutsunderlag för militära chefer för myndighetens lösande av militära uppgifter enligt Försvarsmaktens instruktion, regleringsbrev eller särskilda regeringsbeslut.

4.1.3 Internationellt samarbete

Verksamhet inom totalförsvaret ska kunna bedrivas enskilt och tillsammans med andra, inom och utom landet (Totalförsvaret 2021–2025, prop. 2020/21:30 s. 86–87).

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 bilaterala och multilaterala samarbeten på försvarsområdet med de nordiska och baltiska länderna, liksom med andra länder, t.ex. Frankrike, Storbritannien, Tyskland och USA.

Sverige utvecklar ett särskilt fördjupat försvarssamarbete med Finland. Ett exempel är lagen (2020:782) om operativt militärt stöd mellan Sverige och Finland som trädde i kraft den 15 oktober 2020. Lagen möjliggör för regeringen att, efter begäran från Finland, besluta om att stödja Finland vid kränkningar av finskt territorium, samt att från Finland ta emot militärt stöd vid ett väpnat angrepp mot Sverige eller för att hindra kränkningar av svenskt territorium i fred eller under krig mellan främmande stater.

Försvarsmakten deltar i de internationella samarbeten som 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 effektivare användning av resurser och att öka den operativa förmågan för det svenska försvaret.

4.2 Försvarets radioanstalt

4.2.1 Försvarets radioanstalts uppgifter

Försvarets radioanstalts uppgifter framgår av förordningen (2007:937) med instruktion för Försvarets radioanstalt. I förordningen anges 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 förordningen med instruktion för Försvarets radioanstalt särskilt följa förändringen av signalmiljön i omvärlden, den tekniska utvecklingen och signalskyddet, fortlöpande utveckla den teknik och metodik som behövs för att bedriva verksamheten och utföra matematiska bedömningar av kryptosystem för totalförsvaret (2 §).

Enligt samma förordning ska Försvarets radioanstalt därutöver upprätthålla kompetensen för de nationella behoven i fråga om kryptologi 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 §), samt stödja Försvarsmakten i verksamhet som avser utveckling och vidmakthållande av Försvarsmaktens cyberförsvarsförmåga (3 e §). På uppdrag av Försvarets materielverk får 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 §).

Inom ramen för myndighetens arbete på informationssäkerhetsområdet utvecklar och placerar Försvarets radioanstalt efter begäran 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.

4.2.2 Försvarets radioanstalts informationssäkerhetsverksamhet

Försvarets radioanstalt har, som beskrivs i avsnitt 4.2.1, ett särskilt uppdrag att lämna stöd så att informationssäkerheten kan upprätthållas vid de mest skyddsvärda verksamheterna i Sverige. Försvarets radioanstalt har även till uppgift att tilldela säkra kryptografiska funktioner till ett antal civila myndigheter och organisationer (17 § förordningen [2015:1053] om totalförsvar och höjd beredskap).

För att kunna hantera de allvarligaste it-angreppen mot de mest skyddsvärda verksamheterna använder Försvarets radioanstalt uppgifter som myndigheten har inhämtat genom signalspaning i försvarsunderrättelseverksamhet. 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 Försvarets radioanstalts tekniska detekterings- och varningssystem (TDV). TDV erbjuds de mest skyddsvärda verksamheter som redan har uppnått en egen god informationssäkerhet, ofta med stöd av Försvarets radioanstalt.

4.3 Försvarsmaktens och Försvarets radioanstalts försvarsunderrättelseverksamhet

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

Försvarsunderrättelseverksamhet ska bedrivas av Försvarsmakten, Försvarets radioanstalt, Försvarets materielverk och Totalförsvarets forskningsinstitut. Försvarsunderrättelseverksamheten ska bedrivas till stöd för svensk utrikes-, säkerhets- och försvarspolitik samt i övrigt för kartläggning av yttre hot mot landet. Försvarsunderrättelseverksamhet får endast avse utländska förhållanden. I verksamheten ingår att medverka i svenskt deltagande i internationellt säkerhetssamarbete. Regeringen ansvarar för att 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 4.4.

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.

Information som behandlas inom försvarsunderrättelseverksamheten kan exempelvis avse pågående och tänkbara framtida konflikter, internationella terroristgrupper, cyberhot, massförstörelsevapen samt biografiska underrättelser som avser utländsk militär personal eller andra viktiga befattningshavare.

Försvarsunderrättelseverksamheten tar sikte 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 röjas för 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 har 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 har identifierats, t.ex. kvarvarande oupptäckta hot.

Försvarsunderrättelseverksamheten ska fullgöras genom inhämtning, bearbetning och analys av information samt rapportering till berörda myndigheter (2 § lagen om försvarsunderrättelseverksamhet). Inhämtningen kan vara såväl teknisk som personbaserad. 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 (4 § första stycket lagen om försvarsunderrättelseverksamhet). Om det inte finns hinder enligt andra bestämmelser, får försvarsunderrättelsemyndigheterna emellertid lämna stöd till andra myndigheters brottsbekämpande och brottsförebyggande verksamhet (4 § andra stycket 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 § första stycket lagen om försvarsunderrättelseverksamhet. 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 (En anpassad försvarsunderrättelseverksamhet, prop. 2006/07:63 s. 48).

Försvarsunderrättelsemyndigheterna får etablera och upprätthålla samarbete i underrättelsefrågor med andra länder och internationella organisationer enligt regeringens närmare bestämmande. Samarbetet får ske bara under förutsättning att syftet är att tjäna den svenska statsledningen och det svenska totalförsvaret. De uppgifter som lämnas till andra länder och

internationella organisationer får inte vara till skada för svenska intressen (3 § lagen om försvarsunderrättelseverksamhet och 3 § förordningen om försvarsunderrättelseverksamhet). Myndigheterna ska anmäla frågor om att etablera och upprätthålla samarbetet och om viktiga frågor som uppkommer i samarbetet till Regeringskansliet (Försvarsdepartementet) (4 § förordningen om försvarsunderrättelseverksamhet).

4.4 Försvarets radioanstalts signalspaning i försvarsunderrättelse- och utvecklingsverksamhet

4.4.1 Gällande reglering

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

Signalspaning i försvarsunderrättelseverksamhet får endast 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 typiskt sett informationen och inte den källa som för stunden hanterar eller förmedlar information, som är det centrala vid signalspaning. 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.

All signalspaning i försvarsunderrättelseverksamhet 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 också 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. För att kunna tillgodose uppdragsgivarnas underrättelsebehov behöver Försvarets radioanstalt ingående kunskap om signalmiljön för att på ett effektivt sätt kunna rikta inhämtningskapacitet mot adekvata 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 signaler i elektronisk form därför 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 (1 § tredje stycket lagen om signalspaning i försvarsunderrättelseverksamhet). Utvecklingsverksamheten fyller således inte något självändamål, utan syftar enbart till att etablera och vidmakthålla fortsatt förmåga som är nödvändig för försvarsunderrättelseverksamheten.

Signalspaning i utvecklingsverksamheten inriktas endast av regeringen (4 § andra stycket lagen om signalspaning i försvarsunderrättelseverksamhet) och förutsätter, liksom övrig signalspaning enligt lagen, tillstånd från Försvarsunderrättelsedomstolen.

4.4.2 Internationellt samarbete

Regleringen för internationellt samarbete inom försvarsunderrättelseverksamheten (se avsnitt 4.3) gäller även för Försvarets radioanstalts signalspaning inom den verksamheten. Försvarets radioanstalt får också, enligt regeringens närmare bestämmande, etablera och upprätthålla internationellt signalspaningssamarbete avseende utvecklingsverksamhet, dvs. följa förändringar i signalmiljön i omvärlden, den tekniska

utvecklingen och signalskyddet, samt teknik- och metodikfrågor (9 § lagen om signalspaning i försvarsunderrättelseverksamhet).

En utgångspunkt för internationellt samarbete inom försvarsunderrättelse- och utvecklingsverksamheten är att det ska tjäna statsledningen och det svenska totalförsvaret respektive den nationella säkerheten, och att det inte är till skada för svenska intressen. Försvarets radioanstalt ska anmäla frågor om att etablera och upprätthålla internationellt samarbete till Regeringskansliet (Försvarsdepartementet). Myndigheten ska vidare informera Försvarsdepartementet om viktiga frågor som uppkommer i samarbetet (se 3 § och 4 § första stycket förordningen om försvarsunderrättelseverksamhet och 7 § förordningen om signalspaning i försvarsunderrättelseverksamhet).

4.5 Försvarsmaktens och Försvarets radioanstalts behandling av personuppgifter

4.5.1 Gällande reglering

Försvarsmaktens behandling av personuppgifter inom ramen för försvarsunderrättelseverksamheten och den militära säkerhetstjänsten regleras i lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst och förordningen (2007:260) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst (förkortade FM-PuL och FM-PuF). För Försvarets radioanstalts behandling av personuppgifter inom myndighetens försvarsunderrättelse- och utvecklingsverksamhet gäller lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet och förordningen (2007:261) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet (förkortade 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).

FM-PuL och FRA-PuL är båda självständiga och heltäckande regleringar som ersätter personuppgiftslagen (1998:204) fullt ut inom sina respektive tillämpningsområden (1 kap. 1 § andra stycket FM-PuL och FRA-PuL). Den personuppgiftsbehandling som inte omfattas av FM-PuL och FRA-PuL har reglerats genom personuppgiftslagen. Sedan den 25 maj 2018 gäller personuppgiftslagen fortsatt under en övergångsperiod för Försvarsmakten och Försvarets radioanstalt i sådan verksamhet som inte omfattas av unionsrätten (Ny dataskyddslag, prop. 2017/18:105 s. 171–172).

4.5.2 Exempel på annan reglering som gäller för Försvarsmakten

Patientdatalagen

Patientdatalagen (2008:355) gäller vid vårdgivares behandling av personuppgifter inom hälso- och sjukvården (1 kap. 1 § patientdatalagen). Av 1 kap. 3 § patientdatalagen framgår att med vårdgivare avses även statlig myndighet i fråga om sådan hälso- och sjukvård som myndigheten har ansvar för. Typiskt för statliga vårdgivare är att hälso- och sjukvård inte utgör kärnverksamhet utan bedrivs parallellt med annan verksamhet. Patientdatalagen gäller i de fallen endast i den del av verksamheten som innefattar sådan hälso- och sjukvård som avses i patientdatalagen. Totalförsvarets plikt- och prövningsverk är exempel på en myndighet som bedriver sådan hälso- och sjukvård (Patientdatalag m.m., prop. 2007/08:126 s. 50). Även Försvarsmakten bedriver hälso- och sjukvård vid sina förband i Sverige och i insatser utomlands. Vid personuppgiftsbehandling som Försvarsmakten utför i egenskap av vårdgivare inom hälso- och sjukvården tillämpar myndigheten således patientdatalagen.

Totalförsvarsdatalagen

Totalförsvarsdatalagen (2020:151) ger stöd för bl.a. Försvarsmakten att behandla känsliga personuppgifter om det är absolut nödvändigt vid en utredning om den totalförsvarspliktiges personliga förhållanden som görs enligt 2 kap. 1 § lagen (1994:1809) om totalförsvarsplikt. Försvarsmakten får även med stöd av totalförsvarsdatalagen föra in och rätta personuppgifter om totalförsvarspliktiga i Totalförsvarets plikt- och prövningsverks informationssystem.

Brottsdatalagen

Brottsdatalagen (2018:1177) kan 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. Utförandet av sådana uppgifter kan dock också komma att aktualiseras inom ramen för Försvarsmaktens militära säkerhetstjänst. I 1 kap. 4 § brottsdatalagen anges 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.

4.5.3 Exempel på annan reglering som gäller för Försvarets radioanstalt

Lagen om signalspaning i försvarsunderrättelseverksamhet innehåller vissa bestämmelser som har bäring på Försvarets radioanstalts behandling av personuppgifter, 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 §§).

5 Det grundläggande skyddet för personuppgifter

5.1 Regeringsformen och Europakonventionen

Enligt regeringsformen 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 (2 kap. 6 § andra stycket regeringsformen, förkortad RF). Skyddet får begränsas genom lag men endast för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. En begränsning 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. 20 och 21 §§ RF).

I propositionen En reformerad grundlag 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). Konstitutionsutskottet har i flera lagstiftningsärenden som rört myndigheters personuppgiftsbehandling framhållit att målsättningen bör vara att myndighetsregister med ett stort antal registrerade och särskilt känsligt innehåll ska regleras särskilt i lag (se bl.a. bet. 1990/91:KU11 s. 11 och 1997/98:KU18 s. 43).

Den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) gäller som lag. Enligt artikel 8 i Europakonventionen har var och en rätt till skydd 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 bl.a. den nationella säkerheten och den allmänna säkerheten. Tillämpnings-

området för artikeln omfattar behandling av personuppgifter om privatliv, familjeliv, hem eller korrespondens. 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 sin 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. En lag eller annan föreskrift får inte meddelas i strid med Sveriges åtaganden på grund av Europakonventionen (2 kap. 19 § RF).

5.2 Europarådets dataskyddskonvention

De dataskyddsregler som har antagits inom ramen för Europarådet finns främst i Europarådets konvention om skydd för enskilda vid automatisk databehandling av personuppgifter (ETS 108), den s.k. dataskyddskonventionen. Konventionen, som Sverige har ratificerat och som trädde i kraft den 1 oktober 1985, kompletteras av ett antal av Europarådets ministerkommitté antagna icke-bindande rekommendationer om hur personuppgifter bör behandlas inom olika områden. Dataskyddskonventionen gäller för Europarådets 47 medlemsstater, men även Argentina, Kap Verde, Marocko, Mauritius, Mexiko, 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 (artikel 1 i dataskyddskonventionen).

Dataskyddskonventionen 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. Till sådana kategorier hör personuppgifter som avslöjar ras, politisk tillhörighet, religiös tro eller övertygelse i övrigt, sexualliv samt uppgifter om brott (artikel 6). Dataskyddskonventionen reglerar 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 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). Tilläggsprotokollet innehåller bestämmelser om tillsynsmyndigheter och överföring av personuppgifter till länder som inte är bundna av konventionen. Tilläggsprotokollet, som

Sverige har ratificerat, 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 bara får ske om landet i fråga säkerställer en adekvat skyddsnivå för uppgifterna.

Det grundläggande skyddet vid automatiserad behandling av personuppgifter inom EU regleras numera främst genom dataskyddsförordningen (se avsnitt 5.3). Dataskyddskonventionen är dock alltjämt relevant, särskilt vid behandling av personuppgifter på områden som inte omfattas av EU:s kompetensområde, t.ex. allmän säkerhet och försvar.

Efter en genomförd översyn av dataskyddskonventionen antog Europarådets medlemsstater den 18 maj 2018 ett ändringsprotokoll till konventionen (CETS 223). Ändringsprotokollet träder i kraft när det har ratificerats av Europarådets samtliga 47 medlemsstater. Ändringsprotokollet tillåter också ett delvis ikraftträdande inom en mindre grupp och efter fem år från den dag då det öppnades för undertecknande. Sverige har undertecknat ändringsprotokollet, som den 1 september 2021 hade ratificerats av elva medlemsstater.

5.3 Europeiska unionen

5.3.1 EU-stadgan

Av Europeiska unionens stadga om de grundläggande rättigheterna, förkortad EU-stadgan, 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 EU-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, med beaktande av proportionalitetsprincipen, endast göras om de är nödvändiga och faktiskt svarar mot mål av allmänt samhällsintresse som erkänns av unionen eller behovet av skydd för andra människors rättigheter och friheter.

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

5.3.2 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 gällde inte för behandling av personuppgifter utanför unionsrätten, t.ex. allmän säkerhet, försvar, statens säkerhet och statens verksamhet på straffrättens område. Personuppgiftslagen, genom vilken dataskyddsdirektivet huvudsakligen genomfördes i svensk rätt, gjordes emellertid generellt tillämplig och omfattade således även sådan verksamhet som faller utanför direktivets tillämpningsområde (Personuppgiftslag, prop. 1997/98:44 s. 40). Särreglering i lag eller förordning gällde framför bestämmelserna i personuppgiftslagen.

5.3.3 EU:s dataskyddsförordning

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 inrättades Europeiska dataskyddsstyrelsen med representanter från samtliga EU-länders dataskyddsmyndigheter, däribland Integritetsskyddsmyndigheten (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.

Utöver dataskyddsförordningen gäller sedan den 25 maj 2018 även lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen). Bestämmelserna i EU:s dataskyddsförordning och dataskyddslagen gäller även vid behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av unionsrätten (1 kap. 2 § dataskyddslagen). Europeiska dataskyddsstyrelsen saknar emellertid behörighet inom detta utvidgade tillämpningsområde (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 (1 kap. 3 § dataskyddslagen).

Samtidigt som EU:s dataskyddsförordning och dataskyddslagen trädde i kraft upphävdes personuppgiftslagen. Enligt övergångsbestämmelserna till dataskyddslagen ska personuppgiftslagen dock fortsätta att gälla i sådan verksamhet hos Försvarsmakten och Försvarets radioanstalt som inte omfattas av unionsrätten.

5.3.4 2016 års dataskyddsdirektiv

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 (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 säkerheten.

Direktivet har i huvudsak genomförts genom en ny ramlag, brottsdatalagen. Lagen är subsidiär i förhållande till annan lag eller förordning, vilket möjliggör avvikande bestämmelser i andra författningar.

6 Allmänna utgångspunkter för en ny reglering

6.1 Två nya lagar införs

Regeringens förslag: Det införs en ny lag om behandling av personuppgifter vid Försvarsmakten som ersätter lagen om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst.

Det införs en ny lag om behandling av personuppgifter vid Försvarets radioanstalt som ersätter lagen om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet.

Utredningens förslag överensstämmer med regeringens förslag.

Remissinstanserna: Majoriteten av remissinstanserna, däribland *Datainspektionen*, *Inspektionen för strategiska produkter*, *Migrationsverket*, *Försvarsmakten*, *Försvarets radioanstalt*, *Försvarets materielverk*, *Försvarsunderrättelsedomstolen*, *Totalförsvarets forskningsinstitut* och *Tullverket*, tillstyrker eller invänder inte mot utredningens förslag. *Sveriges advokatsamfund* anser att utredningens förslag inte i tillräcklig grad har beaktat den särskilda problematik som underrättelseverksamhet kan medföra för den personliga integriteten.

Skälen för regeringens förslag

Regeringsformen och krav på reglering i lag

Försvarsmakten och Försvarets radioanstalt bedriver verksamheter som rör Sveriges försvar och säkerhet och har inom sina respektive verksamheter behov av att behandla personuppgifter. Såväl Försvarsmakten som Försvarets radioanstalt behandlar ett stort antal personuppgifter där något samtycke av den registrerade, med hänsyn till karaktären av myndigheternas verksamheter, inte har inhämtats. Inom försvarsunderrättelseverksamheten och Försvarsmaktens militära säkerhetstjänst förekommer kartläggning av enskilda i den mening som avses enligt regeringsformens reglering om skyddet mot betydande intrång i den personliga integriteten (se avsnitt 5.1). Försvarsmaktens och Försvarets radioanstalts försvarsunderrättelseverksamhet får dock endast avse utländska förhållanden. Rätten till skydd mot betydande intrång i den personliga integriteten enligt 2 kap. 6 § andra stycket RF gäller för var och en, dvs. både för svenska medborgare och utlänningar. Kartläggning av t.ex. utländska militära företrädare utanför Sverige omfattas emellertid inte av regeringsformens skydd för den personliga integriteten och krav på lagreglering. Det hindrar inte att lagstiftaren ändå väljer att i lag reglera delar av den personuppgiftsbehandling som ska vara möjlig att utföra i sådan verksamhet. Försvarets radioanstalts utvecklings- och informationssäkerhetsverksamhet är inte av sådant slag att det innebär någon övervakning eller kartläggning av enskilda i regeringsformens mening (se avsnitten 4.2.1 och 4.2.2). Försvarsmaktens behandling av personuppgifter i myndighetens militära säkerhetstjänst får emellertid, i

den utsträckning det saknas samtycke från den registrerade, anses utgöra sådan kartläggning av enskilda.

Grundlagsskyddet mot betydande intrång i den personliga integriteten kan begränsas i lag under förutsättning att begränsningen görs för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle (2 kap. 20 § första stycket 2 och 21 § RF). Det är av grundläggande betydelse i ett demokratiskt samhälle att kunna upprätthålla landets försvar och säkerhet. Försvarsmakten är en central myndighet i detta avseende. För att myndigheten ska kunna fullgöra sitt uppdrag i den militära säkerhetstjänsten behöver den kunna behandla personuppgifter. Det är enligt regeringen därmed fråga om en sådan begränsning som får anses proportionerlig och nödvändig för att tillgodose ett ändamål som är godtagbart i ett demokratiskt samhälle.

Sammantaget anser regeringen att grundläggande bestämmelser för behandlingen av personuppgifter i Försvarsmaktens och Försvarets radioanstalts verksamheter, i likhet med nuvarande ordning, bör regleras i lag. Det är samtidigt olämpligt att tynga lagarna med alltför detaljerade bestämmelser. Lagarna bör därför i lämplig utsträckning kompletteras genom föreskrifter på förordningsnivå.

Två nya lagar bör införas

Utredningens förslag innebär ett flertal ändringar i förhållande till befintlig lagstiftning på området. Det föreslås såväl införande av nya bestämmelser i sak, inbegripet ett utvidgat tillämpningsområde, som redaktionella och språkliga ändringar. Det bör därför införas nya lagar som ersätter nuvarande FM-PuL och FRA-PuL (jfr även avsnitt 17). De nya lagarna bör benämnas lagen om behandling av personuppgifter vid Försvarsmakten och lagen om behandling av personuppgifter vid Försvarets radioanstalt.

De föreslagna nya lagarna bygger i stor utsträckning på FM-PuL och FRA-PuL och har utformats med utgångspunkt från Försvarsmaktens och Försvarets radioanstalts behov av att kunna bedriva sina verksamheter effektivt och med hänsyn till skyddet för enskildas integritet. Till skillnad från *Sveriges advokatsamfund* anser regeringen att även de nya lagarna beaktar skyddet för enskildas personliga integritet på ett väl avvägt sätt.

Lagförslagen och deras förhållande till nuvarande reglering behandlas närmare i det följande.

6.2 Förhållandet till EU:s dataskyddsförordning

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

Förhållandet till EU:s dataskyddsförordning och lagen med kompletterande bestämmelser till EU:s dataskyddsförordning ska framgå av de nya lagarna.

Utredningens förslag överensstämmer delvis med regeringens. I utredningens lagförslag anges endast lagen med kompletterande bestämmelser till EU:s dataskyddsförordning. Utredningens lagförslag

innehåller även en upplysningsbestämmelse om att de föreslagna lagarna inte inskränker myndigheternas skyldighet att lämna ut personuppgifter enligt offentlighetsprincipen.

Remissinstanserna: Flertalet remissinstanser tillstyrker eller invänder inte mot utredningens förslag. *Försvarsmakten* föreslår att även EU:s dataskyddsförordning ska anges uttryckligen i lagarna. *Sveriges advokatsamfund* framhåller vikten av att det klart framgår när de föreslagna lagarna är tillämpliga i förhållande till EU:s dataskyddsförordning. *TCO* anser att de nya lagarnas förhållande till såväl tryckfrihetsförordningen som yttrandefrihetsgrundlagen bör anges i lagarna.

Skälen för regeringens förslag: Försvarsmakten och Försvarets radioanstalt bedriver verksamhet som rör Sveriges försvar och säkerhet. Av fördraget om Europeiska unionen framgår att i synnerhet den nationella säkerheten ska vara varje medlemsstats eget ansvar (artikel 2.4). Uttrycket nationell säkerhet inbegriper bl.a. även försvar.

I EU:s dataskyddsförordning anges att förordningen inte ska tillämpas på behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av unionsrätten (artikel 2.2 a). Av skälen till dataskyddsförordningen framgår att förordningen inte är tillämplig på frågor som rör skyddet av grundläggande rättigheter eller friheter eller det fria flödet av personuppgifter på områden som inte omfattas av unionsrätten, såsom verksamhet rörande nationell säkerhet (skäl 16). Dataskyddsförordningen ska inte heller tillämpas på behandling av personuppgifter som medlemsstaterna utför när de bedriver verksamhet som omfattas av den gemensamma utrikes- och säkerhetspolitiken (artikel 2.2 b). Det framgår således direkt av dataskyddsförordningen att den inte är tillämplig på den behandling av personuppgifter som sker inom Försvarsmaktens och Försvarets radioanstalts verksamheter. Dataskyddsförordningen har dock kommit att få ett utvidgat tillämpningsområde i Sverige. I lagen 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 §).

I propositionen Ny dataskyddslag anför 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 till dataskyddslagen 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. Regeringen återkommer i avsnitten 7 och 8 om vilken personuppgiftsbehandling vid Försvarsmakten och Försvarets radioanstalt som bör omfattas av de nya lagarna.

I sammanhanget bör det framhållas att EU:s dataskyddsförordning bygger på och vidareutvecklar Europarådets dataskyddskonvention som även omfattar nationell säkerhet och försvar. 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 i dataskyddskonventionen). 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). Regeringen bedömer att förslagen i detta lagstiftningsärende är förenliga med dataskyddskonventionen och dess tilläggsprotokoll.

Med utgångspunkt från att de verksamheter Försvarsmakten och Försvarets radioanstalt bedriver till huvudsaklig del ligger utanför unionsrätten bör författningsregleringen i fråga om myndigheternas personuppgiftsbehandling vara heltäckande och utformas så att den gäller exklusivt på de områden som anges i respektive lag inom det aktuella området.

EU:s dataskyddsförordning är direkt tillämplig i Sverige och kompletteras av dataskyddslagen. Det bör, som *Sveriges advokatsamfund* efterfrågar, av de nya lagarna för Försvarsmaktens och Försvarets radioanstalts personuppgiftsbehandling tydligt framgå hur regleringen förhåller sig till EU:s dataskyddsförordning och dataskyddslagen.

I både FM-PuL och FRA-PuL finns en upplysningsbestämmelse om att lagen inte tillämpas i den utsträckning det skulle inskränka skyldigheten enligt 2 kap. tryckfrihetsförordningen att lämna ut personuppgifter. Regeringen anser, till skillnad från utredningen, att det inte finns något behov av att föra in motsvarande reglering i de nya lagarna.

6.3 Syftet med de nya lagarna

Regeringens förslag: Syftet med de nya lagarna är 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 förslag överensstämmer med regeringens.

Remissinstanserna: Flertalet remissinstanser tillstyrker eller invänder inte mot utredningens förslag.

Skälen för regeringens förslag: Syftet med nuvarande reglering är 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). Personuppgiftsbehandlingen ska vara nödvändig (1 kap. 8 §) och fler personuppgifter får inte behandlas än som är nödvändigt med hänsyn till ändamålen med behandlingen (1 kap. 6 § 6).

Även de nya lagarna bör innehålla bestämmelser om syftet med lagarna där såväl kravet på ändamålsenlighet som intresset att skydda fysiska personers fri- och rättigheter framgår. Utredningen föreslår mot den bakgrunden att syftet med de nya 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.

Regeringen anser i likhet med majoriteten av remissinstanserna att utredningens förslag är väl avvägt och bör genomföras. Lagtexten bör utformas i enlighet med detta.

6.4 De nya lagarnas tillämpningsområden

6.4.1 Tillämpningsområdet för lagen om behandling av personuppgifter vid Försvarsmakten

Regeringens förslag: Lagen om behandling av personuppgifter vid Försvarsmakten ska gälla vid behandling av personuppgifter i myndighetens verksamhet som rör Sveriges försvar och säkerhet samt internationellt försvars- och säkerhetssamarbete.

Lagen ska gälla för sådan behandling av personuppgifter som är helt eller delvis automatiserad. Den ska också gälla personuppgifter som ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda rutiner.

Utredningens förslag överensstämmer i sak med regeringens.

Remissinstanserna: *Försvarsmakten* anser att en särskild författningsreglering för Försvarsmaktens personuppgiftsbehandling kommer att leda till bättre förutsättningar för att bedriva verksamhet och i förlängningen bidra till en ökning av den operativa förmågan, och att ett överskådligt och förenklat regelverk också bidrar till ett förbättrat skydd för den som personuppgiften rör. *Sveriges advokatsamfund* anser att utredningens förslag till utformning kan väcka frågor om lagens räckvidd i förhållande till Försvarsmaktens verksamhet.

Skälen för regeringens förslag: Frågor om försvar och nationell säkerhet omfattas som utgångspunkt inte av unionsrätten. Enligt ikraftträdande- och övergångsbestämmelserna till dataskyddslagen ska personuppgiftslagen under en övergångsperiod fortsätta att gälla i sådan verksamhet hos Försvarsmakten som inte omfattas av unionsrätten och som inte för närvarande regleras i FM-PuL.

Försvarsmakten har flera verksamhetsuppdrag, men det grundläggande uppdraget är att upprätthålla och utveckla ett militärt försvar som ytterst kan möta ett väpnat angrepp. Det grundläggande uppdraget, som ligger utanför EU-rätten, har en nära koppling till Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst. I dessa verksamheter är frågan om personuppgiftsbehandling enligt nuvarande ordning särreglerad genom FM-PuL. I propositionen Lag om försvarsunderrättelseverksamhet som låg till grund för lagen om försvarsunderrättelseverksamhet, anförs att det ligger 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).

I militär säkerhetstjänst och försvarsunderrättelseverksamhet tillämpas för närvarande FM-PuL, men inom logistik, samband och personaladministration tillämpar Försvarsmakten personuppgiftslagen. Omvärldsbevakning, operationsplanering, civil-militär samverkan, samt taktisk och operativ underrättelsetjänst bedrivs med stöd av antingen FM-PuL eller personuppgiftslagen beroende på var inom myndigheten personuppgifterna hanteras och i vilket syfte. En personuppgift kopplad till exempelvis en specifik operation kan därför behandlas med stöd av olika personuppgiftsregelverk i samma databehandlingssystem.

Den reglering av personuppgiftsbehandling som nu gäller för Försvarsmakten, med två tillämpliga regelverk beroende på var inom myndigheten uppgiften för tillfället behandlas, försvårar informationsutbytet mellan system och verksamheter. Det leder till att effektiviteten inom Försvarsmakten och därmed den samlade operativa effekten riskerar att försämras. Regeringen anser att en mer sammanhållen reglering skulle motverka detta.

Vid tillkomsten av FM-PuL 2007 överfördes regelverket för den personuppgiftsbehandling som utfördes i myndighetens försvarsunderrättelseverksamhet och militära säkerhetstjänst, och som sedan 2001 hade reglerats särskilt i förordning, till lag. Sedan 2014 sker det en utveckling av det militära försvaret av Sverige och Försvarsmaktens operativa förmåga (Försvarspolitisk inriktning – Sveriges försvar 2016–2020, prop. 2014/15:109 och Totalförsvaret 2021–2025, prop. 2020/21:30). Vidare har en återuppbyggnad av totalförsvaret med en sammanhängande totalförsvarsplanering inletts. Denna utveckling och Försvarsmaktens särskilda ställning i totalförsvaret i allmänhet och det militära försvaret i synnerhet leder till att det nu finns skäl att – i förhållande till nuvarande ordning – utvidga tillämpningsområdet för den nya särreglering som föreslås gälla vid Försvarsmaktens behandling av personuppgifter. Försvarsmaktens verksamhet omfattas typiskt sett inte av unionsrätten.

Regeringen anser, i likhet med utredningen, att den nya lagen så långt det är möjligt och lämpligt bör följa strukturen i EU-regleringen och annan svensk särreglering på dataskyddsområdet som ligger utanför unionsrätten. Detta är en fördel i tillämpningshänseende för såväl Försvarsmakten som tillsyns- och kontrollmyndigheterna, liksom för enskilda ur ett integritetsskyddsperspektiv.

Som *Lagrådet* uppmärksammar bör det i fråga om tillämpningsområdet klart framgå av den nya lagen vilka verksamheter inom Försvarsmakten som lagen omfattar. Den nya lagen bör således omfatta behandlingen av personuppgifter i Försvarsmaktens verksamhet som rör Sveriges försvar och säkerhet samt internationellt försvars- och säkerhetssamarbete. Regeringen ser inte att det finns någon risk för att en sådan utformning kan leda till tillämpningssvårigheter av det slag som *Sveriges advokatsamfund* befarar.

Nuvarande reglering är tillämplig vid personuppgiftsbehandling 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. Manuell behandling i t.ex. register omfattas alltså av regelverket om uppgifterna är

tillgängliga för sökning eller sammanställning enligt mer än ett kriterium. Som utredningen föreslår bör den nya lagen ha motsvarande tillämpningsområde.

6.4.2 Tillämpningsområdet för lagen om behandling av personuppgifter vid Försvarets radioanstalt

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

Lagen ska gälla för sådan behandling av personuppgifter som är helt eller delvis automatiserad. Den ska också gälla personuppgifter som ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda rutiner.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: *Försvarets radioanstalt* instämmer i utredningens förslag. *Datainspektionen* delar utredningens bedömning att den nya lagen även bör omfatta informationssäkerhetsverksamhet.

Skälen för regeringens förslag: Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet syftar till att upprätthålla Sveriges försvar och säkerhet. Verksamheten omfattas inte av unionsrätten.

I Försvarets radioanstalts informationssäkerhetsverksamhet tillämpas. personuppgiftslagen vid behandling av personuppgifter (se avsnitt 4.5.1). Syftet med informationssäkerhetsverksamheten vid Försvarets radioanstalt är att stödja verksamheter som har betydelse för Sveriges säkerhet. Den omfattas därför inte av unionsrätten. Informationssäkerhetsverksamheten har vidare ett nära samband med signalspaning i försvarsunderrättelseverksamhet. Enligt lagen om signalspaning i försvarsunderrättelseverksamhet får signalspaning ske i syfte att kartlägga bl.a. allvarliga yttre hot mot samhällets infrastruktur (1 § andra stycket 5). Möjligheten till utbyte av information mellan signalspaningen och informationssäkerhetsverksamheten utgör ett viktigt verktyg för att kunna upprätthålla Sveriges säkerhet. Med hänsyn till att verksamhetsområdena till sin karaktär är nära sammanlänkade, anser regeringen att starka skäl talar för att behandlingen av personuppgifter bör regleras i ett gemensamt regelverk. Som utredningen, med instämmande av *Försvarets radioanstalt* och *Datainspektionen,* föreslår bör därför Försvarets radioanstalts behandling av personuppgifter i informationssäkerhetsverksamheten också regleras i den nya lagen.

Nuvarande särreglering är tillämplig vid personuppgiftsbehandling 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. Manuell behandling i t.ex. register omfattas alltså av regelverket om uppgifterna är tillgängliga för sökning eller sammanställning enligt mer än

ett kriterium. Den nya lagen bör, som utredningen föreslår, utformas på motsvarande sätt.

6.5 Vissa ord och uttryck i lagarna ska definieras

Regeringens förslag: Vissa ord och uttryck som används i de nya lagarna ska definieras.

Utredningens förslag överensstämmer i huvudsak med regeringens. Utredningen föreslår inte någon definition av ordet registrerad.

Remissinstanserna: *Försvarsmakten* föreslår att definitionen av uppgiftssamling för myndighetens vidkommande avgränsas till att avse Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst. *Datainspektionen* anser att definitionen av dataskyddsombud även bör omfatta juridiska personer och att det för personuppgiftsbiträde inte ska finnas ett uttryckligt krav på skriftligt avtal. *Forum för dataskydd* ifrågasätter utredningens förslag när det gäller dataskyddsombudets uppgifter. *Sveriges advokatsamfund* anser att uttryck i de föreslagna lagarna bör definieras på samma sätt som i EU:s dataskyddsförordning.

Skälen för regeringens förslag

Behovet av definitioner

Sedan FM-PuL:s och FRA-PuL:s tillkomst 2007 har bl.a. den tekniska utvecklingen påverkat innebörden av vissa ord och uttryck som används i de lagarna. Utvecklingen innebär också att vissa ord och uttryck 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 ord och uttryck både i lagstiftning som omfattas av EU-rätten och i lagstiftning som inte gör det. I den utsträckning som samma ord och uttryck används, bör de i möjligaste mån ha samma betydelse i även sådan lagstiftning som reglerar verksamhet utanför EU-rättens tillämpningsområde. Om ord och uttryck har samma innebörd i lagarna på dataskyddsområdet kan missförstånd undvikas.

Enligt *Sveriges advokatsamfund* bör uttrycken i de nya lagarna definieras på samma sätt som i EU:s dataskyddsförordning.

Som behandlas i avsnitt 6.2 är de föreslagna lagarna fristående från dataskyddsförordningen. Regeringen anser därför inte att en sådan ordning är lämplig. Det är emellertid önskvärt att lagar om behandlingen av personuppgifter utformas på ett enhetligt sätt, bl.a. i fråga om definitioner av vissa förekommande ord och uttryck. I det följande behandlas vissa centrala definitioner i de nya lagarna.

Regeringen återkommer till definitionerna av personuppgiftsansvarig (avsnitt 11.1), dataskyddsombud (avsnitt 11.4) och personuppgiftsbiträde (avsnitt 11.5.1).

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.

Regeringen 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 ändring, framtagning, läsning, användning, utlämnande, spridning eller tillhandahållande på annat sätt, justering, sammanföring, begränsning, radering eller förstöring.

Den föreslagna lydelsen innebär endast vissa språkliga skillnader jämfört med EU:s dataskyddsförordning och vissa ändringar i de angivna exemplen jämfört med nuvarande FM-PuL och FRA-PuL. Orden återvinning, inhämtande, blockering och utplåning tas bort, medan strukturering, framtagning, läsning, justering, sammanföring, begränsning och radering tillkommer.

I fråga om orden radering, förstöring och utplåning kan noteras att radering och förstöring finns med i definitionen av personuppgiftsbehandling i EU:s dataskyddsförordning (artikel 4), men någon närmare förklaring till vad radering respektive förstöring innebär finns inte utöver att radering kopplas till rätten att bli bortglömd (artikel 17). Radering eller rätten att bli bortglömd antyder att radering enligt dataskyddsförordningen innebär att personuppgifterna ska tas bort på ett sådant sätt att informationen inte kan återskapas vid senare tillfälle (Ny dataskyddslag, SOU 2017:39 s. 317), dvs. samma betydelse som utplåna enligt nuvarande FM-PuL och FRA-PuL (prop. 2006/07:46 s. 90). Ordet radering kan även jämföras med förstöring, som är det ord som används i lagen om signalspaning i försvarsunderrättelseverksamhet. Data ska alltså raderas på ett sådant sätt att den inte kan återskapas. Enligt regeringens mening hindrar en sådan utformning av bestämmelsen inte en fortsatt teknisk utveckling av hur detta genomförs i praktiken, utan att den rättsliga innebörden påverkas.

Begränsning kan jämföras med blockering, som används i FM-PuL och FRA PuL. Enligt bestämmelserna utgör 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. tryckfrihetsförordningen (1 kap. 4 §). Definitionen stämmer väl överens med beskrivningen av ordet 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 typisk åtgärd kan vara att avskilja personuppgifterna 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 personuppgifterna.

Biometriska uppgifter

Biometri är en samlingsbeteckning för sådan automatiserad teknik som syftar till att identifiera en person eller avgöra om en påstådd identitet är riktig. Den baseras på mätning av fysiska karaktärsdrag hos den som ska identifieras (Fingeravtryck i pass, prop. 2008/09:132 s. 6–7). När det gäller pass är det framför allt mönster av fingeravtryck, ansiktsgeometri och ögats iris som används, men även regnbågshinna, näthinna, röst, hand, blodkärl, dna eller gång går att använda. Gemensamt för teknikerna är att kroppen mäts elektroniskt. Biometriska uppgifter är den information som kan tas fram ur ett biometriskt underlag. Dessa uppgifter kan användas för att skapa en referensmall eller för att jämföra med tidigare lagrade referensmallar i syfte att kontrollera en persons identitet. I EU:s dataskyddsförordning anges ansiktsbilder som ett exempel på biometriska uppgifter i definitionen av sådana uppgifter. Det kan leda tanken till att vanliga fotografier och filmer skulle omfattas av definitionen. Om de inte bearbetas tekniskt genom en särskild metod som syftar till identifiering faller de utanför definitionen. Om de däremot bearbetas i exempelvis ett ansiktsigenkänningsprogram så att det går att identifiera personer på bilden eller filmen omfattas de av definitionen. Här kan även anmärkas att personuppgifter, t.ex. fingeravtryck, som förekommer i ett utlåtande som baseras på en teknisk bearbetning av biometriska uppgifter inte i sig utgör biometriska uppgifter.

FM-PuL och FRA-PuL saknar en definition av biometriska uppgifter. Uttrycket biometriska uppgifter bör, som utredningen föreslår, 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 identifiering av personen i fråga.

Genetiska uppgifter

Genetiska uppgifter definieras inte i nuvarande FM-PuL och FRA-PuL. I de nya lagarna bör genetiska uppgifter definieras som personuppgifter som rör en persons nedärvda eller förvärvade genetiska kännetecken och som framför allt härrör från analys av ett spår av eller ett biologiskt prov från personen i fråga.

Genetiska uppgifter handlar framför allt om information som kan tas fram vid dna-analyser, men även motsvarande information som tas fram genom andra analyser omfattas. Genetiska uppgifter behandlas vid dna-analyser för att ta fram dna-profiler eller forensiska uppslag. Eftersom nedärvda eller förvärvade genetiska kännetecken för en fysisk person kan framgå av ett spår omfattas även analys av spåren, trots att de då inte går att härleda till en identifierad person. Själva dna-profilen är endast en sifferkombination och därmed ingen genetisk uppgift. Den är däremot en biometrisk uppgift, eftersom det är möjligt att med hjälp av den unikt identifiera en person.

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 bör definieras som den till vilken personuppgifter lämnas ut, med undantag av en myndighet som med stöd av författning utövar tillsyn, kontroll eller revision. I förhållande till nuvarande FM-PuL och FRA-PuL bör en ändring av endast språklig karaktär göras.

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.

Personuppgift bör i de nya lagarna definieras som varje upplysning om en identifierad eller identifierbar fysisk person som är i livet. Den nya lydelsen är inte avsedd att innebära någon ändring i sak, men gör enligt regeringens mening definitionen mer enhetlig med övriga lagar på området för personuppgiftsbehandling.

Registrerad

Registrerad definieras i FM-PuL och FRA-PuL som den som en personuppgift avser. Utredningen föreslår inte någon definition av registrerad i de nya lagarna. Enligt EU:s dataskyddsförordning är en registrerad en identifierad eller identifierbar fysisk person. I likhet med annan särskild lagstiftning om personuppgiftsbehandling bör registrerad definieras som den fysiska person som personuppgiften gäller.

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.

Tredje man bör i förhållande till nuvarande reglering ändras till tredje part i enlighet med utredningens förslag. Tredje part bör definieras som någon annan än den registrerade, den personuppgiftsansvarige, dataskyddsombudet, personuppgiftsbiträdet och sådana personer som under den personuppgiftsansvariges eller personuppgiftsbiträdets direkta ansvar har rätt att behandla personuppgifter.

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 samma definition ska införas i de nya lagarna med den ändringen att uttrycket används gemensamt byts ut mot är gemensamt tillgängliga.

Försvarsmakten anför att definitionen av uppgiftssamling för Försvarsmaktens vidkommande bör avse endast myndighetens försvarsunderrättelseverksamhet och militära säkerhetstjänst.

Regeringen anser att definitionen av ordet uppgiftssamling lämpligen bör vara densamma i de nya lagarna. Det hindrar inte att regleringen kan skilja sig åt i fråga om i vilka fall personuppgifter som är gemensamt tillgängliga vid Försvarsmakten respektive Försvarets radioanstalt ska behandlas i uppgiftssamlingar (se avsnitt 9). Utredningens förslag till definition bör därför genomföras.

7 Ändamål för behandlingen av personuppgifter

7.1 Behandling får bara ske för särskilda, uttryckligt angivna och berättigade ändamål

Regeringens 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.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Flertalet remissinstanser tillstyrker eller invänder inte mot utredningens förslag. *Juridiska fakultetsstyrelsen vid Lunds universitet* lyfter frågan om inte ändamålen bör preciseras närmare och dokumenteras innan insamlingen påbörjas. *Sveriges advokatsamfund* förordar en uttömmande uppräkning av de ytterligare ändamål som skulle kunna komma i fråga.

Skälen för regeringens förslag

Behandling för särskilda, uttryckligt angivna och berättigade ändamål

Den omständigheten att viss behandling är rättsligt grundad innebär inte att vilka personuppgifter som helst får behandlas eller att det får göras på valfritt sätt. Den personuppgiftsansvarige måste också iaktta övriga krav som gäller för behandling av personuppgifter.

Av FM-PuL och FRA-PuL framgår att Försvarsmakten respektive Försvarets radioanstalt ska se till att personuppgifter bara samlas in för särskilda, uttryckligt angivna och berättigade ändamål och att personuppgifter inte behandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in (1 kap. 6 § 3 och 4). Regeringen anser att liknande bestämmelser bör föras in i de nya lagarna.

Att ändamålen ska vara särskilda innebär att de måste vara tillräckligt specificerade för att ge ledning för bedömningen av vilka uppgifter som är adekvata och relevanta för den aktuella behandlingen och för att det ska

kunna avgöras att inte fler uppgifter än nödvändigt behandlas. Något hinder mot att ange flera parallella ändamål för behandlingen finns inte. Ändamålen ska anges uttryckligen redan när personuppgifterna samlas in. Till skillnad från *Juridiska fakultetsstyrelsen vid Lunds universitet* ser regeringen inget behov av att i de nya lagarna ytterligare precisera de föreslagna ändamålen för Försvarsmaktens och Försvarets radioanstalts personuppgiftsbehandling.

Att ändamålen ska vara berättigade innebär att det ska finnas en koppling till myndighetens reglerade verksamhet som utgör den rättsliga grunden. Personuppgifter får således inte behandlas för ett ändamål som inte är berättigat i förhållande till verksamheten. Genom att det i stor utsträckning är reglerat vilken personuppgiftsbehandling som kan aktualiseras vid Försvarsmakten och Försvarets radioanstalt har lagstiftaren redan tagit ställning till att personuppgiftsbehandlingen är berättigad i de fallen. Det är dock inte bara när personuppgifter samlas in som det ska finnas ett särskilt, uttryckligt angivet och berättigat ändamål för behandlingen. Motsvarande krav gäller även för varje åtgärd som vidtas med de insamlade uppgifterna.

Juridiska fakultetsstyrelsen vid Lunds universitet lyfter frågan om det bör ställas krav på dokumentation innan en behandling av personuppgifter påbörjas.

Det är viktigt att kunna kontrollera för vilket eller vilka ändamål personuppgifter behandlas oavsett i vilken verksamhet behandlingen görs. Både av hänsyn till verksamheten och till den personliga integriteten är det därför enligt regeringens mening viktigt att det framgår för vilket ändamål en personuppgift behandlas. Från integritetssynpunkt har det betydelse bl.a. för möjligheterna att genom tekniska förfaranden eller administrativa bestämmelser kunna styra åtkomsten till vissa uppgifter.

Att ändamålet med behandlingen framgår är vidare en viktig faktor för att en tillsynsmyndighet ska kunna kontrollera om viss behandling är berättigad och utförs i enlighet med lagens bestämmelser. Information om ändamålet med behandlingen behövs också för att de tjänstemän som får tillgång till personuppgifterna ska kunna värdera personuppgifterna korrekt och använda sig av dem på ett effektivt och lagenligt sätt. Informationen behövs bl.a. för att kunna ta ställning till om uppgiften får och bör behandlas för ett nytt ändamål.

Med hänsyn till den verksamhet som Försvarsmakten och Försvarets radioanstalt bedriver bör det emellertid redan av sammanhanget typiskt sett framgå för vilka ändamål en viss personuppgift behandlas. Av detta följer att verksamhetens karaktär i sig innebär en avgränsning av vilka personuppgifter som behandlas. Regeringen anser att detta är en från integritetssynpunkt tillfredsställande ordning och ser därför inte behov av en sådan ordning som Juridiska fakultetsstyrelsen vid Lunds universitet efterfrågar.

Med anledning av *Sveriges advokatsamfund* tveksamhet till sekundära ändamål kan regeringen konstatera att sekundära ändamål och finalitetsprincipen är vedertagna inom dataskyddsområdet och de föreslagna bestämmelserna ger ett tydligt ändamålsstöd för sådan personuppgiftsbehandling. Reglering avseende sekundära ändamål finns t.ex. i totalförsvarsdatalagen och kustbevakningslagen (2019:429).

Advokatsamfundet förordar även att det i de nya lagarna införs en bestämmelse om när personuppgifter ska kunna behandlas för nya ändamål som motsvarar brottsdatalagens reglering. Regeringen noterar att kraven på nödvändighet och proportionalitet i brottsdatalagen har sin grund i 2016 års dataskyddsdirektiv och att direktivets krav inte gäller för de verksamheter som är aktuella i det här lagstiftningsarbetet. Enligt regeringens mening saknas behov av sådan reglering i de nya lagarna.

7.2 Försvarsmakten

7.2.1 Försvar och säkerhet

Regeringens förslag: Personuppgifter får behandlas i Försvarsmaktens verksamhet om behandlingen är nödvändig 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, kollektivavtal eller annat avtal, eller ett särskilt beslut där regeringen har gett myndigheten i uppdrag att utföra uppgiften.

Ändamål för Försvarsmaktens behandling av personuppgifter i myndighetens försvarsunderrättelseverksamhet och militära säkerhetstjänst bör anges i särskilda bestämmelser.

Utredningens förslag överensstämmer i huvudsak med regeringens. Utredningen använder uttrycket rättslig grund.

Remissinstanserna: *Försvarsmakten* framhåller vikten av en samlad reglering av myndighetens personuppgiftsbehandling och att ordet ändamål är vanligt förekommande i dataskyddslagstiftningar, till skillnad från uttrycket rättslig grund som utredningen föreslår. *Datainspektionen* anser att administrativ verksamhet bör antingen särregleras eller behandlas i ett särskilt kapitel i den nya lagen. *Statens inspektion för försvarsunderrättelseverksamheten* efterfrågar ett klargörande om behandling av personuppgifter i försvarsunderrättelseverksamheten och den militära säkerhetstjänsten även ska kunna ske med stöd av bestämmelsen om Sveriges försvar och säkerhet.

Skälen för regeringens förslag

Personuppgiftsbehandling i verksamhet som rör Sveriges försvar och säkerhet

Regeringen föreslår att den nya lagen för Försvarsmaktens behandling av personuppgifter ska få ett bredare tillämpningsområde jämfört med vad som gäller enligt nuvarande ordning (avsnitt 6.4.1). Detta behöver ges stöd genom tydliga ändamål i den nya lagen. I enlighet med utredningens förslag bör således den nya lagen innehålla en ändamålsbestämmelse som anger att personuppgifter få 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 har gett myndigheten i uppdrag att ansvara för uppgiften.

I utredningens lagförslag anges inte kollektivavtal eller annat avtal som uttryckliga stöd för behandlingen av personuppgifter. Enligt dataskyddslagen får personuppgifter behandlas med stöd av artikel 6.1 c i EU:s dataskyddsförordning om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna fullgöra en rättslig förpliktelse som t.ex. följer av kollektivavtal (2 kap. 1 §). Av dataskyddsförordningen följer att personuppgifter också får behandlas om det är nödvändigt för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås (artikel 6.1 b).

Med hänsyn till det bredare tillämpningsområde som den nya lagen för Försvarsmakten föreslås få kommer även personuppgifter inom myndighetens personaladministrativa verksamhet att behandlas med stöd av den nya lagen (se vidare nedan). Det bredare tillämpningsområdet inbegriper även Försvarsmaktens behandling av personuppgifter som föranleds av myndighetens kontakter med bl.a. leverantörer vid upphandling, markägare vid upplåtelse av mark i samband med Försvarsmaktens övningar och fodervärdar för Försvarsmaktens tjänstehundar. Regeringen anser att det i den nya lagen bör tydliggöras att Försvarsmakten får behandla personuppgifter med stöd av kollektivavtal eller annat avtal, om behandlingen är nödvändig för att planera, förbereda och genomföra verksamhet som rör Sveriges försvar och säkerhet (jfr prop. 2017/18:105 s. 51–52). Utredningens lagförslag bör justeras i enlighet med detta.

Regeringen noterar att utredningens förslag innehåller såväl uttrycken rättslig grund som ändamål för när behandling av personuppgifter ska vara tillåten. Rättslig grund är ett uttryck som företrädesvis används i den särskilda dataskyddsreglering som finns inom det brottsbekämpande området. FM-PuL och FRA-PuL, innehåller i stället bestämmelser om primära och sekundära ändamål. Detta gäller även för andra författningar, som t.ex. totalförsvarsdatalagen och kustbevakningsdatalagen.

Regeringen ser ett värde för tillämpningen att i den nya lagen behålla det vedertagna ordet ändamål och föreslår därför att det ordet ska användas i den nya lagen.

Lagrådet invänder inte mot den valda terminologin, men efterfrågar en ökad tydlighet när det gäller hur bestämmelserna om vissa ändamål förhåller sig till regleringen i fråga om andra ändamål enligt den nya lagen. Lagrådet föreslår även en annan författningsteknisk lösning.

De rättsliga grunderna för Försvarsmaktens behandling av personuppgifter finns i de regelverk som ligger till grund för myndighetens verksamheter. Ur ett tillämpningsperspektiv är det väsentligt att den nya lagen innehåller tydliga ändamålsbestämmelser. Detta innebär enligt regeringen inte att det alltid är nödvändigt att i en ändamålsbestämmelse ange den eller de författningar som ligger till grund för den aktuella verksamheten eller att i en sådan bestämmelse ange att en viss verksamhet förutsätter stöd i lag, förordning eller en annan rättslig grund.

Ur ett rättstillämpningsperspektiv framstår Lagrådets förslag till författningsteknisk lösning, enligt regeringens mening, inte som mer

ändamålsenligt och tydligt. Regeringen väljer därför att behålla lagrådsremissens förslag.

Internationellt försvars- och säkerhetssamarbete

Internationellt samarbete på försvars- och säkerhetsområdet utgör en viktig del i upprätthållandet av Sveriges försvar och säkerhet. Försvarsmakten bedriver internationellt försvars- och säkerhetssamarbete enligt regeringens bestämmande. Samarbete sker t.ex. inom det nordiska försvarssamarbetet Nordefco, men också med Nato och inom EU och FN. Sverige har bilaterala försvarssamarbeten med bl.a. Frankrike, Storbritannien, Tyskland och USA, i vilka Försvarsmakten deltar. Försvarsmakten deltar även i internationella fredsfrämjande och humanitära insatser, samt i underrättelsesamarbeten inom ramen för exempelvis EU.

Försvarsmaktens personuppgiftsbehandling som aktualiseras inom det internationella samarbetet, är en del av Sveriges försvar och säkerhet och omfattas därmed av den nya lagen. Behandlingen bör stödjas av ett tydligt ändamål. I likhet med utredningen föreslår regeringen att Försvarsmakten bör få behandla personuppgifter 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.

Även vid deltagande i internationella militära insatser eller vid andra uppdrag i utlandet som Försvarsmaktens personal deltar i, kan kollektivavtal eller avtal med t.ex. en leverantör utgöra grund för en nödvändig behandling av personuppgifter inom Försvarsmakten. Utredningens lagförslag bör justeras i enlighet med detta.

Som *Statens inspektion för försvarsunderrättelseverksamheten* framhåller utgör Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst en del i Sveriges försvar och säkerhet. Med hänsyn till dessa verksamheters särskilda karaktär och att de enligt nuvarande ordning regleras särskilt i FM-PuL bedömer regeringen, i likhet med utredningen, att Försvarsmaktens behandling av personuppgifter inom myndighetens försvarsunderrättelseverksamhet och militära säkerhetstjänst även i den nya lagen bör regleras i särskilda ändamålsbestämmelser. Detta bör komma till uttryck i den nya lagen.

Ska regleringen även omfatta Försvarsmaktens personaladministrativa verksamhet?

Utredningen föreslår att den nya lagen även ska omfatta Försvarsmaktens personaladministrativa verksamhet. *Datainspektionen* anser att administrativ verksamhet bör antingen särregleras eller behandlas i ett särskilt kapitel i den nya lagen.

Regeringen konstaterar, i likhet med Datainspektionen, att utredningens förslag att inbegripa personaladministrativ verksamhet i tillämpningsområdet för den nya lagen skiljer sig från vad som gäller för övriga myndigheter, vars verksamhet i och för sig ligger utanför unionsrätten. I den lag som gäller för Säkerhetspolisens verksamhet har inte den personaladministrativa verksamheten inkluderats (Ny lag om

Säkerhetspolisens behandling av personuppgifter, prop. 2018/19:163 s. 54). I fråga om Försvarets radioanstalt föreslås inte heller en sådan lösning som inbegriper den personaladministrativa verksamheten (se avsnitt 7.3.1). Försvarsmaktens militära förmåga och utvecklingen av densamma är beroende av myndighetens personalförsörjning. Med hänsyn till Försvarsmaktens huvuduppgift, som är att militärt försvara Sverige, och de tydliga kopplingar som finns mellan myndighetens krigsorganisation och personaladministrativa verksamhet anser regeringen att lagen här även behöver omfatta Försvarsmaktens personaladministrativa verksamhet. Någon praktisk åtskillnad mellan dessa uppgifter är nämligen inte möjlig att göra.

Utöver ändamålsbestämmelsen om Sveriges försvar och säkerhet och internationellt försvars- och säkerhetssamarbete föreslås även en ändamålsbestämmelse för behandling av personuppgifter om det är nödvändigt för bl.a. Försvarsmaktens ärendehandläggning (avsnitt 7.2.5). Även den nya lagens bestämmelser om t.ex. känsliga personuppgifter och författningsenlig och korrekt behandling och säkerhet för personuppgifter kommer att vara tillämpliga i myndighetens personaladministrativa verksamhet. Regeringen bedömer att ytterligare bestämmelser inte krävs. För denna verksamhet, liksom för myndighetens verksamhet i övrigt, gäller att en bedömning om hanteringen rör personuppgifter med koppling till verksamhet som rör försvar och säkerhet eller internationellt försvars- och säkerhetssamarbete krävs och styr tillämpningen.

7.2.2 Försvarsmaktens försvarsunderrättelseverksamhet

Regeringens förslag: Personuppgifter får behandlas i Försvarsmaktens försvarsunderrättelseverksamhet om det är nödvändigt för att bedriva den verksamhet som anges i lagen om försvarsunderrättelseverksamhet.

De personuppgifter som Försvarsmakten har fått tillgång till i sin försvarsunderrättelseverksamhet får fortsätta behandlas i den verksamheten, om det behövs för att fullfölja den. Detta gäller dock endast om inte något annat följer av den nya lagen eller en förordning som har meddelats i anslutning till den lagen.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: *Datainspektionen* ifrågasätter inte att det kan finnas ett behov att ta bort det krav på preciserad inriktning som gäller enligt nuvarande lagstiftning för att kunna bedriva en effektiv underrättelseverksamhet, men anser att behovet behöver vägas mot vad lagstiftaren tidigare har framfört som skäl för att införa begränsningen. Enligt *Statens inspektion för försvarsunderrättelseverksamheten* kommer ett borttaget krav på anknytning till en preciserad inriktning vid personuppgiftsbehandling sannolikt att leda till att fler personuppgifter kommer att behandlas och därmed medföra en risk för ökat integritetsintrång för den enskilde.

Skälen för regeringens förslag: Försvarsmakten får enligt nuvarande ordning behandla personuppgifter om det är nödvändigt för att bedriva den

verksamhet som anges i lagen om försvarsunderrättelseverksamhet (1 kap. 8 § första stycket FM-PuL).

I enlighet med utredningens förslag bör en motsvarande bestämmelse införas i den nya lagen.

Enligt nuvarande reglering 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 (1 kap. 8 § andra stycket FM-PuL). Utredningen föreslår att ett sådant krav inte ska införas i den nya lagen, men föreslår att personuppgifter som Försvarsmakten har fått tillgång till i sin försvarsunderrättelseverksamhet fortsatt ska få behandlas i den verksamheten, om det behövs för att fullfölja den. Detta ska dock endast gälla om inte något annat följer av den nya lagen eller en förordning som har meddelats i anslutning till lagen.

Regeringen konstaterar att försvarsunderrättelseverksamhet huvudsakligen är framåtsyftande. I sådan verksamhet kartläggs företeelser i syfte att kunna förvarna om bl.a. avsikter, aktiviteter och hot till stöd för att ge de inriktande myndigheterna ett förbättrat kunskapsläge. 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 som observeras emellertid ofta sättas in i ett kontextuellt och historiskt sammanhang. Först därefter kan bedömningar om underrättelserelevans göras. Det som observeras behöver således analyseras och jämföras med tidigare observationer. För vissa företeelser behöver sådana jämförelser kunna göras med observationer som har gjorts långt tillbaka i tiden, inte sällan 10–20 år tillbaka.

Försvarsunderrättelseverksamhet förutsätter ett beslut om inriktning från regeringen. Inom ramen för sådan inriktning får de myndigheter som regeringen bestämmer ange en närmare inriktning av verksamheten (1 § andra stycket lagen om försvarsunderrättelseverksamhet). Vad som avses med preciserad inriktning anges inte i FM-PuL. Försvarsmakten tar fram en inhämtandeplan för verksamhetens utförande som preciserar inriktningen. I planen gör myndigheten de prioriteringar som den anser vara nödvändiga för att avgränsa myndighetens verksamhet inom försvarsunderrättelseområdet.

Inriktningarna och planeringen utgör avgränsningar av behandlingen av personuppgifter på så sätt att de anger underrättelsebehoven. Det är dock inte möjligt att med ledning av inriktningarna och planeringen i detalj avgöra vilken personuppgiftsbehandling som kan vara och bli nödvändig. Mot denna bakgrund anser regeringen, i likhet med utredningen, att krav på anknytning till en preciserad inriktning inte bör införas i den nya lagen.

Sett till det särskilda behov som finns att fortsatt kunna behandla insamlade personuppgifter inom försvarsunderrättelseverksamheten, bör den nya lagen även ge uttryck för att personuppgifter som Försvarsmakten har fått tillgång till i sin försvarsunderrättelseverksamhet ska få fortsätta behandlas i den verksamheten, om det behövs för att fullfölja den. En förutsättning för detta bör vara att något annat inte följer av den nya lagen eller i en förordning som har meddelats i anslutning till lagen.

Enligt *Datainspektionen* kan det finnas en risk för att förslaget i denna del möjliggör att Försvarsmakten även kan behandla personuppgifter som

inte har inhämtats i enlighet med lagstiftningen. Med hänsyn till den tydliga ram som lagen om försvarsunderrättelseverksamhet ger, liksom den nu föreslagna lagen om Försvarsmaktens behandling av personuppgifter, ser regeringen inte någon sådan risk.

Som *Statens inspektion för försvarsunderrättelseverksamheten* framhåller kan tidigare inhämtade personuppgifter väntas komma att fortsatt behandlas i större utsträckning jämfört med nuvarande ordning. Regeringen bedömer att de tydliga behov som föranleder en sådan ordning överväger det begränsade integritetsintrång som en fortsatt behandling innebär. Det är, på motsvarande sätt som enligt nuvarande ordning, den försvarsunderrättelseverksamhet som ska och får bedrivas med stöd av lagen om försvarsunderrättelseverksamhet som ytterst sätter gränserna.

7.2.3 Militär säkerhetstjänst

Regeringens 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 klarlägga verksamhet som innefattar hot mot Sveriges säkerhet eller för att vidta åtgärder som hindrar eller försvårar säkerhetshotande verksamhet.

Personuppgifter får behandlas för de angivna ändamålen endast om

1. personuppgifterna 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 enligt motsvarande äldre föreskrifter,
2. personuppgifterna är nödvändiga för att kartlägga underrättelseverksamhet riktad mot Försvarsmakten och dess säkerhetsintressen,
3. personuppgifterna är nödvändiga för att kartlägga annan säkerhetshotande verksamhet än som avses i 1 och som innefattar brott eller åsidosättande av skyldigheter i anställning hos Försvarsmakten, och det finns särskilda skäl till att uppgiften ska behandlas,
4. personuppgifterna är nödvändiga för att bedöma om en person som har lämnat uppgifter om säkerhetshotande verksamhet är trovärdig, eller
5. personuppgifterna är nödvändiga för att genomföra säkerhetsprövning enligt säkerhetsskyddslagen (2018:585) eller för att utföra en uppgift som rör säkerhetsskydd.

Personuppgifter som behandlas för att upptäcka, förebygga och avvärja säkerhetshotande verksamhet som riktas mot Försvarsmakten och dess säkerhetsintressen ska förses med upplysning om på vilken av de angivna grunderna uppgiften behandlas.

Om behandlingen av en personuppgift motiveras av något annat än ett antagande om att en person 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 en 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 ett 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.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: *Datainspektionen* ifrågasätter utredningens förslag som enligt myndigheten innebär att fler personuppgifter kan komma att behandlas inom ramen för den militära säkerhetstjänsten. Övriga remissinstanser yttrar sig inte särskilt i denna del.

Skälen för regeringens förslag: Enligt nuvarande ordning får Försvarsmakten behandla personuppgifter i den militära säkerhetstjänsten. Behandling får ske i verksamhet som syftar till 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. Behandling får också ske om det är nödvändigt för att vidta åtgärder som hindrar eller försvårar säkerhetshotande verksamhet (1 kap. 9 § FM-PuL). De beskrivna ändamålen avser Försvarsmaktens säkerhetsunderrättelsetjänst respektive säkerhetsskyddstjänst (prop. 2006/07:46 s. 25).

I FM-PuL ställs vissa krav för behandlingen av personuppgifter i den militära säkerhetstjänsten. En behandling av personuppgifter är endast tillåten om uppgifterna ger grundad anledning att anta att en person 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. Behandling är vidare tillåten om uppgifterna ger grundad anledning att anta att en person har utövat eller kan komma att utöva annan underrättelseverksamhet riktad mot Försvarsmakten och dess säkerhetsintressen eller att personen utövar annan säkerhetshotande verksamhet och som innefattar brott eller åsidosättande av åligganden i anställning hos Försvarsmakten, och det finns särskilda skäl till att uppgifterna behandlas.

Försvarsmakten får enligt gällande rätt även behandla personuppgifter om den berörda personen har lämnat uppgifter om säkerhetshotande verksamhet och uppgifterna är nödvändiga för att bedöma personens trovärdighet eller sådana uppgifter som avser information som har framkommit i samband med att en person har genomgått registerkontroll eller särskild personutredning enligt säkerhetsskyddslagen.

Personuppgifter som behandlas ska förses med upplysning om på vilken grund uppgiften behandlas. Om behandlingen av en personuppgift föranleds av något annat än antagande om att en person 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 i syfte att klarlägga hotande verksamhet mot Försvarsmakten och dess säkerhetsintressen ska i förekommande fall förses med en upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak (1 kap. 10 § FM-PuL).

Utredningen föreslår att motsvarande bestämmelser, med vissa justeringar, bör införas i den nya lagen för Försvarsmakten. En skillnad är att uttrycken registerkontroll eller särskild personutredning ersätts med ordet säkerhetsprövning. På så sätt omfattas alla delar som ingår i en säkerhetsprövning enligt säkerhetsskyddslagen.

Utredningen föreslår vidare att personuppgifter ska få behandlas om uppgifterna är nödvändiga för att kartlägga verksamhet som kan hota rikets säkerhet eller terroristbrott enligt 2 § lagen om straff för terroristbrott eller enligt motsvarande äldre föreskrifter, underrättelseverksamhet riktad mot Försvarsmakten och dess säkerhetsintressen. Utredningen föreslår att detsamma ska gälla i fråga om annan säkerhetshotande verksamhet än brott som kan hota Sveriges säkerhet eller terroristbrott enligt 2 § lagen om straff för terroristbrott eller enligt motsvarande äldre föreskrifter och som innefattar brott eller åsidosättande av åligganden i anställning hos Försvarsmakten, och det finns särskilda skäl till att uppgiften ska behandlas.

Datainspektionen ifrågasätter utredningens förslag i denna del som enligt myndigheten kan leda till att fler personuppgifter kan komma att behandlas inom ramen för den militära säkerhetstjänsten.

Regeringen anser att utredningens förslag på ett lämpligt sätt speglar Försvarsmaktens verksamhetsuppdrag för den militära säkerhetstjänsten. Någon ändring i sak i fråga om vilka personuppgifter som får behandlas är dock inte avsedd. I enlighet med vad som gäller enligt nuvarande ordning kommer det även fortsatt att krävas särskilda skäl för att Försvarsmakten ska få behandla vissa personuppgifter. Detta gäller för personuppgifter som är nödvändiga för att kartlägga annan säkerhetshotande verksamhet än sådan verksamhet som innefattar brott som kan hota Sveriges säkerhet eller terroristbrott enligt nuvarande eller tidigare lagstiftning, och som innefattar brott eller åsidosättande av skyldigheter i anställning hos Försvarsmakten. Det 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 krävs 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. 70–71).

Regeringen föreslår en motsvarighet till nuvarande reglering om Försvarsmaktens behandling av personuppgifter inom myndighetens militära säkerhetstjänst, med utredningens föreslagna justeringar, ska föras in i den nya lagen.

7.2.4 Signalkontrollverksamhet

Regeringens förslag: Personuppgifter som ingår i eller har uppkommit i samband med användning av totalförsvarets telekommunikations- och informationssystem får behandlas i den militära säkerhetstjänsten för att förhindra obehörig insyn i och påverkan av dessa system. Det gäller även känsliga personuppgifter, personnummer och samordningsnummer samt personuppgifter, om den registrerade har lämnat sitt uttryckliga samtycke till behandling eller på ett tydligt sätt har offentliggjort uppgifterna.

Behandling som särskilt syftar till att identifiera en person får dock endast utföras om det är nödvändigt för att kartlägga

– verksamhet som innefattar brott som kan hota Sveriges säkerhet eller terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott eller enligt motsvarande äldre föreskrifter,

– underrättelseverksamhet som riktas mot Försvarsmakten och dess säkerhetsintressen, eller

– annan säkerhetshotande verksamhet än brott som kan hota Sveriges säkerhet eller terroristbrott och som innefattar brott eller åsidosättande av skyldigheter i anställning hos Försvarsmakten, och det finns särskilda skäl till att uppgiften ska behandlas.

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

Utredningens förslag överensstämmer delvis med regeringens. Utredningen föreslår inte att Försvarsmakten ska föra en förteckning över de behandlingar som särskilt syftar till att identifiera en person och de uppgifter som utgjort anledningen till behandlingen.

Remissinstanserna yttrar sig inte särskilt över utredningens förslag.

Skälen för regeringens förslag: Enligt nuvarande ordning 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 personnummer. Försvarsmakten ska föra en förteckning över de behandlingar som särskilt syftar till att identifiera en person och de uppgifter som utgjort anledningen till behandlingen. En sådan förteckning har till syfte att möjliggöra kontroll i efterhand av grunden för att en behandling utförts i syfte att identifiera en person (1 kap. 11 § FM-PuL).

Utredningen föreslår att en motsvarande bestämmelse ska tas in i den nya lagen med den skillnaden att behandling av personuppgifter för detta ändamål även får avse sådana uppgifter som den enskilde har gjort offentliga (se avsnitt 8.4). Enligt utredningens förslag ska det inte heller ställas krav på en förteckning. Som skäl för detta anför utredningen att Försvarsmakten är skyldig att spara sådana uppgifter redan på grund av bl.a. lagens krav om rättslig grund och loggning. Enligt utredningens förslag har även dataskyddsombudet till uppgift att föra förteckning över myndighetens behandlingar.

Regeringen konstaterar att den förteckning som i vissa fall ska föras inom ramen för signalkontrollverksamheten avser en specifik behandling

som syftar till att identifiera en person och de uppgifter som utgjort anledningen till behandlingen. Ifrågavarande förteckning skiljer sig därför från de förteckningar över myndighetens personuppgiftsbehandling som den personuppgiftsansvarige ska föra (se avsnitt 11.4). Med hänsyn till förteckningens värde ur ett integritetsskyddsperspektiv bör ett motsvarande krav även införas i den nya lagen. Med den justeringen bör utredningens förslag genomföras.

7.2.5 Ärendehandläggning och liknande uppgifter

Regeringens förslag: Försvarsmakten får behandla personuppgifter om det är nödvändigt för diarieföring, arkivering eller handläggning av ett ärende eller för att utföra andra liknande uppgifter som myndigheten har.

Utredningens förslag överensstämmer i huvudsak med regeringens. Utredningen använder uttrycket rättslig grund.

Remissinstanserna yttrar sig inte särskilt över utredningens förslag.

Skälen för regeringens förslag: Tillämpningsområdet för den nya lagen inbegriper även administrativ verksamhet hos Försvarsmakten. Enligt nuvarande ordning regleras detta i personuppgiftslagen och FM-PuL saknar därför bestämmelser om diarieföring, arkivering eller handläggning av ärenden eller andra liknande uppgifter som Försvarsmakten har. Regeringen anser, i likhet med utredningen, att det av den nya lagen bör framgå att myndigheten även får behandla personuppgifter kopplade till sådana åtgärder.

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. Detsamma gäller de arkiverade handlingarna. Ärendehandläggningen vid myndigheten kan t.ex. avse skadeståndsärenden, tillträdesärenden där en annan stat begär 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. Myndigheten är också skyldig att t.ex. besvara frågor rörande Sveriges försvar och att kommunicera med anställda eller värnpliktiga i frågor som rör deras tjänst. Det förekommer också ärenden om utvärdering av den egna verksamheten såsom tidredovisning, lönesättning och sjuktal.

Som utredningen föreslår bör den behandling av personuppgifter som uppkommer i bl.a. dessa verksamheter omfattas av den nya lagen. I avsnitt 7.2.1 behandlas även vissa bestämmelser i övrigt som kommer att bli tillämpliga i Försvarsmaktens administrativa verksamhet.

7.3 Försvarets radioanstalt

7.3.1 Försvarets radioanstalts försvarsunderrättelseverksamhet

Regeringens förslag: Personuppgifter får behandlas i Försvarets radioanstalts försvarsunderrättelseverksamhet om det är nödvändigt för att bedriva den verksamhet som anges i lagen om försvarsunderrättelseverksamhet och lagen om signalspaning i försvarsunderrättelseverksamhet.

De personuppgifter som Försvarets radioanstalt har fått tillgång till i sin försvarsunderrättelseverksamhet får även fortsätta behandlas i den verksamheten, om det behövs för att fullgöra den. Detta gäller dock endast om inte något annat följer av den nya lagen eller en förordning som har meddelats i anslutning till lagen.

Personuppgifter som Försvarets radioanstalt behandlar i försvarsunderrättelseverksamheten får myndigheten även behandla 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 om försvarsunderrättelseverksamhet och lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet,
3. i Försvarets radioanstalts utvecklingsverksamhet för det ändamål som gäller för den verksamheten,
4. i Försvarets radioanstalts informationssäkerhetsverksamhet för det ändamål som gäller för den verksamheten, eller
5. för att biträda andra myndigheter i den utsträckning det följer av lag eller förordning eller om regeringen har beslutat om det i ett enskilt fall.

Utredningens förslag överensstämmer i huvudsak med regeringens.

Remissinstanserna: *Datainspektionen* anser att behovet av att ta bort nuvarande krav på preciserad inriktning för att kunna bedriva en effektiv underrättelseverksamhet bör vägas mot lagstiftarens skäl för att införa begränsningen. Datainspektionen ställer sig vidare tveksam till utredningens bedömning att förslaget till sekundära ändamålsbestämmelser utgör en kodifiering av gällande finalitetsprincip. *Statens inspektion för försvarsunderrättelseverksamheten* anser att det är sannolikt att ett borttaget krav på en anknytning till en preciserad inriktning vid personuppgiftsbehandling leder till att fler personuppgifter behandlas och därmed medför en risk för ökat integritetsintrång för den enskilde. Myndigheten pekar vidare på risken för ett ökat integritetsintrång för den enskilde då utbyten av personuppgifter mellan försvarsunderrättelseverksamheten och informationssäkerhetsverksamheten innebär att uppgifterna kommer fler till del.

Behandling av personuppgifter i försvarsunderrättelseverksamheten

Försvarets radioanstalt får enligt nuvarande ordning behandla personuppgifter om det är nödvändigt för att bedriva den verksamhet som anges i lagen om försvarsunderrättelseverksamhet (1 kap. 8 § första stycket FRA-PuL). Försvarets radioanstalt bedriver signalspaning i försvarsunderrättelseverksamhet enligt lagen om signalspaning i försvarsunderrättelseverksamhet.

I enlighet med utredningens förslag bör en ändamålsbestämmelse ge uttryck för att Försvarets radioanstalt får behandla personuppgifter i sin försvarsunderrättelseverksamhet om det är nödvändigt för att bedriva den verksamhet som anges i lagen om försvarsunderrättelseverksamhet och lagen om signalspaning i försvarsunderrättelseverksamhet.

På motsvarande sätt som gäller för FM-PuL, finns även i FRA-PuL ett krav på att uppgifter om en person endast får behandlas om personen har anknytning till en preciserad inriktning för försvarsunderrättelseverksamheten och behandlingen är nödvändig för att fullfölja den inriktningen (1 kap. 8 § andra stycket FRA-PuL).

Utredningen föreslår, i likhet med sitt förslag till ny lag för Försvarsmaktens personuppgiftsbehandling, att kopplingen enligt nuvarande ordning till en preciserad inriktning ska tas bort för Försvarets radioanstalts behandling av personuppgifter (jfr avsnitt 7.2.2). Inom Försvarets radioanstalt finns, på motsvarande sätt som för Försvarsmakten, ett behov av att i försvarsunderrättelseverksamheten behandla äldre information, inbegripet personuppgifter, för att man ska kunna förstå och bedöma den underrättelsemässiga relevansen av sådant som sker i nuläget. Utredningens förslag ger också ett stöd för behandling av personuppgifter 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 *Datainspektionen* kan det finnas en risk för att förslaget i denna del möjliggör Försvarets radioanstalt även kan behandla personuppgifter som inte har samlats in i enlighet med lagstiftningen. Med hänsyn till den tydliga ram som lagen om försvarsunderrättelseverksamhet och lagen om signalspaning i försvarsunderrättelseverksamhet ger, ser regeringen inte någon sådan risk. Utredningens förslag i denna del bör därför genomföras.

Som *Statens inspektion försvarsunderrättelseverksamheten* uppmärksammar kan förslaget komma att medföra att tidigare inhämtade personuppgifter behandlas i större utsträckning jämfört med nuvarande reglering. Regeringen bedömer att det allmännas behov av en sådan ordning överväger det begränsade integritetsintrång för enskilda som en fortsatt behandling innebär. Det är den försvarsunderrättelseverksamhet som ska och får bedrivas med stöd av lagen om försvarsunderrättelseverksamhet och lagen om signalspaning i försvarsunderrättelseverksamhet som ytterst sätter gränserna.

Lagrådet anser att det kan finnas skäl att tydliggöra att de ändamål som förslaget innehåller i fråga om Försvarets radioanstalts behandling av personuppgifter i utvecklingsverksamheten och informationssäkerhetsverksamheten utgör särskilda bestämmelser för försvarsunderrättelse-

verksamheten. Lagrådet föreslår därför att det i den nya lagen införs en särskild upplysningsbestämmelse om detta. Regeringen anser dock att utformningen enligt lagrådsremissens förslag är tillräckligt tydligt ur ett rättstillämpningsperspektiv och därför bör stå kvar.

Behandling av personuppgifter för sekundära ändamål

Vidarebehandling av personuppgifter för vissa andra ändamål än de ursprungliga ändamålen får göras med stöd av 1 kap. 6 § 4 FRA-PuL. Bestämmelsen ger uttryck för finalitetsprincipen, dvs. att den personuppgiftsansvarige har möjlighet att fortsatt behandla insamlade personuppgifter så länge de inte behandlas för något ändamål som är oförenligt med det för vilket de samlades in.

Som utredningen föreslår bör det i den nya lagen införas preciserade ändamålsbestämmelser om i vilka fall Försvarets radioanstalt får behandla personuppgifter för ett annat ändamål än för det ändamål för vilket personuppgifterna har samlats in. En sådan ordning skapar enligt regeringens mening ökad tydlighet och innebär ett stärkt integritetsskydd. Försvarets radioanstalts verksamhetsansvar är av sådan tydligt avgränsad omfattning att ett införande av sekundära ändamål är lämpligt när det gäller behandling av personuppgifter i myndighetens försvarsunderrättelse- och utvecklingsverksamhet, samt informationssäkerhetsverksamhet, vilket utredningen också föreslår. Regeringen anser, till skillnad från *Datainspektionen*, att det inte finns skäl att ifrågasätta utredningens bedömning att förslaget innebär en kodifiering av finalitetsprincipen och en möjlighet att i tydliggörande bestämmelser reglera personuppgiftsbehandling för sekundära ändamål. Förslaget har uppenbara fördelar ur ett integritetsskyddsperspektiv och motsvarande reglering om behandling av personuppgifter för sekundära ändamål finns även i andra regelverk om personuppgiftsbehandling, t.ex. totalförsvarsdatalagen.

Det bör således av den nya lagen framgå att personuppgifter som behandlas i Försvarets radioanstalts försvarsunderrättelseverksamhet även får behandlas i myndighetens utvecklingsverksamhet om det är nödvändigt för att tillhandahålla information som behövs i utvecklingsverksamheten för de ändamål som gäller för den verksamheten. Informationsverksamheten är nära knuten till vissa delar av försvarsunderrättelseverksamheten vilket ger unika möjligheter till ökad säkerhet på it-området. Av den anledningen är det viktigt att personuppgifter som behandlas i försvarsunderrättelseverksamheten också får behandlas i informationssäkerhetsverksamheten enligt de ändamål som anges för den verksamheten. Försvarets radioanstalt bör även få behandla personuppgifter i syfte att kunna lämna information till andra i verksamhet hos berörda myndigheter som avses i 2 § lagen om försvarsunderrättelseverksamhet, vid samarbete med andra länder och internationella organisationer enligt lagen om försvarsunderrättelseverksamhet och lagen om signalspaning i försvarsunderrättelseverksamhet, samt vid biträde till andra myndigheter i den utsträckning det följer av lag eller förordning eller om regeringen har beslutat om det i ett enskilt fall.

Den föreslagna regleringen innebär således att personuppgiftsbehandling för vissa sekundära ändamål uttryckligen anges i lagen i stället

för att som tidigare enbart grundas på den lagstadgade finalitetsprincipen. Finalitetsprincipen, som även föreslås komma till uttryck i den nya lagen, gäller därutöver.

Förslaget i denna del är enligt regeringen att betrakta som ett tydliggörande i förhållande till befintlig bestämmelse i FRA-PuL om finalitetsprincipen. Med hänsyn till de behov av skyddsåtgärder som finns på försvarsunderrättelse- och informationssäkerhetsområdet kan det, som *Statens inspektion försvarsunderrättelseverksamheten* påpekar, förväntas att utbytet av personuppgifter inom Försvarets radioanstalt kan komma att öka. Som behandlas i avsnitt 11.3.2 ska det även fortsatt framgå av lag att tillgången till personuppgifter ska begränsas till vad var och en behöver för att fullgöra sina arbetsuppgifter. Det begränsade intrång i den personliga integriteten som förslaget innebär får anses vara acceptabelt i förhållande till verksamheternas syfte.

Försvarets radioanstalts personaladministrativa verksamhet omfattas inte av den nya lagen

Utredningen föreslår inte att den nya lagen ska omfatta även personaladministrativ verksamhet hos Försvarets radioanstalt. Regeringen anser att en sådan ordning i och för sig skulle kunna övervägas. Det saknas dock beredningsunderlag för att göra detta inom ramen för nu aktuellt lagstiftningsprojekt.

7.3.2 Utvecklingsverksamhet

Regeringens 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 Försvarets radioanstalts utvecklingsverksamhet får myndigheten även behandla om det är nödvändigt för att tillhandahålla information som behövs

1. med anledning av samverkan med annan i fråga om utvecklingsverksamhet,
2. med anledning av samarbete om utvecklingsverksamhet med utländsk underrättelse- eller säkerhetstjänst enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet,
3. i Försvarets radioanstalts försvarsunderrättelseverksamhet för det ändamål som gäller för den verksamheten,
4. i Försvarets radioanstalts informationssäkerhetsverksamhet för det ändamål som gäller för den verksamheten, eller
5. för att biträda andra myndigheter i den utsträckning det följer av lag eller förordning eller om regeringen har beslutat om det i ett enskilt fall.

Utredningens förslag överensstämmer i huvudsak med regeringens.

Remissinstanserna: *Försvarets radioanstalt* tillstyrker utredningens förslag. Övriga remissinstanser yttrar sig inte över utredningens förslag.

Skälen för regeringens förslag

Behandling av personuppgifter i utvecklingsverksamheten

Försvarets radioanstalt ska enligt sin instruktion 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, som anger att signaler i elektronisk form får inhämtas vid signalspaning för dessa syften. Myndigheten ska enligt sin instruktion även 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 för närvarande i 1 kap. 9 § FRA-PuL. Enligt bestämmelsen får personuppgifter behandlas av Försvarets radioanstalt om det är nödvändigt för att följa förändringar av signalmiljön i omvärlden, den tekniska utvecklingen och signalskyddet, och fortlöpande utveckla den teknik och metodik som behövs för att bedriva verksamheten. I enlighet med utredningens förslag bör en motsvarande bestämmelse införas i den nya lagen.

Behandling av personuppgifter för sekundära ändamål

Från integritetsskyddssynpunkt är det en fördel att så långt som möjligt precisera i vilka fall personuppgiftsbehandling får ske för annat ändamål än det ändamål enligt vilket uppgifterna har samlats in (jfr avsnitt 7.3.1).

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 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 vilket uppgifterna samlas in att uppgifterna också behandlas för att tillhandahålla information som behövs i försvarsunderrättelseverksamheten. Detta bör som utredningen föreslår komma till uttryck i den nya lagen.

Försvarets radioanstalts utvecklingsverksamhet har också betydelse för myndighetens 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.

Den föreslagna regleringen innebär således att personuppgiftsbehandling för vissa sekundära ändamål uttryckligen anges i lagen i stället för att som tidigare enbart grundas på den lagstadgade finalitetsprincipen. Finalitetsprincipen, som även föreslås komma till uttryck i den nya lagen, gäller därutöver.

7.3.3 Informationssäkerhetsverksamhet

Regeringens 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 beslut av regeringen i ett enskilt fall.

Personuppgifter som behandlas i Försvarets radioanstalts informationssäkerhetsverksamhet får myndigheten även behandla om det är nödvändigt för att tillhandahålla information som behövs

1. i verksamhet hos den som tar emot informationssäkerhetsuppgifter,
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 har beslutat om det i ett enskilt fall,
3. i Försvarets radioanstalts försvarsunderrättelseverksamhet när det gäller att kartlägga allvarliga yttre hot mot samhällets infrastruktur och främmande underrättelseverksamhet mot svenska intressen, samt
4. i Försvarets radioanstalts utvecklingsverksamhet för det ändamål som gäller för den verksamheten.

Utredningens förslag överensstämmer i huvudsak med regeringens

Remissinstanserna: *Försvarets radioanstalt* tillstyrker utredningens förslag. *Statens inspektion för försvarsunderrättelseverksamheten* påminner om att myndigheten inte har fått till uppgift att granska Försvarets radioanstalts informationssäkerhetsverksamhet.

Skälen för regeringens förslag

Behandling av personuppgifter i informationssäkerhetsverksamheten

Försvarets radioanstalt har i uppdrag att vara statens resurs för teknisk informationssäkerhet och ska ha hög kompetens inom informationssäkerhetsområdet. Myndigheten får 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 (4 § förordningen med instruktion för Försvarets radioanstalt och 17 § förordningen om totalförsvar och höjd beredskap). Försvarets radioanstalts stöd innebär bl.a. att Försvarets

radioanstalt på uppdragsgivarens begäran söker efter och analyserar brister i säkerheten i datorsystemen. Ett annat exempel på stöd är Försvarets radioanstalts tekniska detekterings- och varningssystem som beskrivs i avsnitt 4.2.2.

Den personuppgiftsbehandling som Försvarets radioanstalt genomför i egenskap av personuppgiftsansvarig inom ramen för informationssäkerhetsverksamheten omfattas inte av FRA-PuL. Regeringen anser i likhet med utredningen att det i den nya lagen bör införas en bestämmelse som anger 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. Försvarets radioanstalts uppgift att lämna stöd till andra verksamheter ska följa av lag eller förordning eller beslut av regeringen i ett enskilt fall. Härigenom får Försvarets radioanstalt en samlad reglering som gäller oavsett om myndigheten har inlett en behandling av personuppgifter i sin försvarsunderrättelseverksamhet eller inom informationssäkerhetsverksamheten.

Som *Statens inspektion för försvarsunderrättelseverksamheten* uppmärksammar har myndigheten inte till uppgift att granska Försvarets radioanstalts informationssäkerhetsverksamhet. Regeringen vill med anledning av detta understryka att Statens inspektion för försvarsunderrättelseverksamheten har getts en särskild och betydelsefull uppgift att kontrollera den försvarsunderrättelseverksamhet som bedrivs av berörda myndigheter och Försvarets radioanstalts signalspaning i försvarsunderrättelseverksamhet. Statens inspektion för försvarsunderrättelseverksamheten ska också särskilt granska den personuppgiftsbehandling som sker i dessa verksamheter hos Försvarets radioanstalt.

Integritetsskyddsmyndigheten ska enligt regeringens förslag ha tillsynsansvaret för Försvarets radioanstalts personuppgiftsbehandling i informationssäkerhetsverksamheten (se avsnitt 13). Detta påverkar inte Statens inspektion för försvarsunderrättelseverksamhetens möjlighet att granska personuppgifter som behandlas i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet. Granskningsansvaret för Försvarets radioanstalts behandling av personuppgifter inom den verksamheten gäller oaktat för vilket ändamål som personuppgifterna ursprungligen har samlats in.

Behandling av personuppgifter för sekundära ändamål

Från integritetsskyddssynpunkt är det en fördel att så långt som möjligt precisera i vilka fall Försvarets radioanstalt får behandla personuppgifter för andra ändamål än det för vilket uppgifterna har samlats in (jfr avsnitt 7.3.1). Om personuppgifter hämtas in inom ramen för Försvarets radioanstalts informationssäkerhetsverksamhet bör dessa i enlighet med utredningens förslag kunna behandlas även om det är nödvändigt för att tillhandahålla information som behövs hos den som tar emot uppgifter om informationssäkerhet.

Enligt *Lagrådet* bör det övervägas om inte lagförslaget i denna del bör få en tydligare och mer avgränsad utformning. Regeringen konstaterar att mottagaren av uppgifter om informationssäkerhet kan vara en annan

myndighet eller en annan aktör för vars räkning Försvarets radioanstalt har utfört aktiva it-kontroller eller installerat ett tekniskt detekterings- och varningssystem. Försvarets radioanstalts stöd till vissa skyddsvärda aktörer på informationssäkerhetsområdet är av stor betydelse för Sveriges säkerhet, men är också av avgränsad omfattning.

Med hänsyn till detta anser regeringen att lagrådsremissens lagförslag är både ändamålsenligt och tillräckligt tydligt. Det bör därför stå kvar.

Vidare bör behandling 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. Som utredningen föreslår bör behandling av personuppgifter i dessa fall få ske enbart i den utsträckning det följer av lag eller förordning eller om regeringen har beslutat om det i ett enskilt fall.

En nära samverkan mellan försvarsunderrättelseverksamheten och informationssäkerhetsverksamheten är av stor betydelse. För försvarsunderrättelseverksamheten 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. Regeringen anser att personuppgifter därför även bör få behandlas om det är nödvändigt för att tillhandahålla information av detta slag. Försvarets radioanstalt har därvid att förhålla sig till de bestämmelser som gäller för försvarsunderrättelseverksamheten.

Försvarets radioanstalts informationssäkerhetsverksamhet är även av betydelse för myndighetens utvecklingsverksamhet. Personuppgifter som Försvarets radioanstalt får behandla i myndighetens informationssäkerhetsverksamhet bör därför även få behandlas om det är nödvändigt för att tillhandahålla information som behövs i utvecklingsverksamheten.

Den föreslagna regleringen innebär således att personuppgiftsbehandling för vissa sekundära ändamål uttryckligen regleras i lag, i stället för att, som hittills, hanteras i enlighet med finalitetsprincipen. Avsikten är att skapa ökad tydlighet. Finalitetsprincipen gäller därutöver.

7.4 Behandling av allmänt tillgänglig information

Regeringens förslag: Försvarsmakten får behandla personuppgifter som utgör allmänt tillgänglig information om det är nödvändigt för myndighetens försvarsunderrättelseverksamhet eller militära säkerhetstjänst, eller vid planering, förberedelse och genomförande av annan verksamhet som rör Sveriges försvar och säkerhet eller internationellt försvars- och säkerhetssamarbete.

Försvarets radioanstalt får behandla personuppgifter som utgör allmänt tillgänglig information om det är nödvändigt för de ändamål som anges för försvarsunderrättelse- och utvecklingsverksamheten och informationssäkerhetsverksamheten.

Utredningens förslag överensstämmer i sak med regeringens.

Remissinstanserna: *Försvarets radioanstalt* välkomnar utredningens förslag.

Skälen för regeringens förslag: För att kunna bedriva en effektiv försvarsunderrättelseverksamhet behöver Försvarsmakten och Försvarets

radioanstalt, utöver den information som myndigheterna inhämtar genom särskilda metoder, också god tillgång till allmänt tillgänglig information. Därigenom kan den på särskilt sätt inhämtade informationen sättas in i sitt rätta sammanhang på ett bättre sätt. Av intresse i sammanhanget är information som utgörs av personuppgifter som kan påträffas vid sökning på internet eller vid sökningar i öppna databaser. Uppgifterna kan vara tillgängliga såväl på kommersiell grund som utan avgift. Gemensamt för dem är att de är publikt tillgängliga. Det kan t.ex. vara fallet när en abonnent på något sätt har samtyckt till att uppgifterna finns med i elektroniska telefonkataloger eller förteckningar över ip-adresser i olika länder. Sådana databaser anskaffas och läggs 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 ovan beskrivna sättet. För Försvarsmaktens del har myndigheten även ett sådant behov inom den militära säkerhetstjänsten. Behovet förekommer även när det gäller planering, förberedelse och genomförande av verksamhet som avser Sveriges försvar och säkerhet eller internationellt försvars- och säkerhetssamarbete.

Utöver de syften för sådan behandling inom 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. Detta är en nödvändighet då inhämtning enligt lagen om signalspaning i försvarsunderrättelseverksamhet inte får avse signaler mellan en avsändare och en mottagare som båda befinner sig i Sverige (2 a §). 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 är ett nödvändigt verktyg för att i möjligaste mån minska omfattningen av den inhämtning som annars kan ske.

Även inom Försvarets radioanstalts utvecklingsverksamhet 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 lagen om signalspaning i försvarsunderrättelseverksamhet, varvid behandling av allmänt tillgängliga personuppgifter kan bidra till att minska omfattningen av sådan inhämtning som inte är tillåten enligt den lagen.

Försvarets radioanstalt kan också inom sin informationssäkerhetsverksamhet behöva behandla allmänt tillgängliga personuppgifter. 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.

Antalet personuppgifter i Försvarsmaktens och Försvarets radioanstalts referensdatabaser kan bli mycket stort. Även om personuppgifterna är allmänt tillgängliga innebär det stora antalet personuppgifter en form av integritetsintrång. De föreslagna ändamål som behandlas i avsnitten 7.2 och 7.3 omfattas i och för sig av den ovan beskrivna behandlingen av personuppgifter. För att undvika oklarheter i rättstillämpningen bör stödet för sådan behandling dock komma till tydligt uttryck i lagtexten i linje med utredningens förslag.

7.5 Behandling för vetenskapliga, statistiska eller historiska ändamål

Regeringens förslag: Försvarsmakten och Försvarets radioanstalt får behandla personuppgifter för vetenskapliga, statistiska eller historiska ändamål inom de föreslagna lagarnas tillämpningsområden.

Utredningens förslag överensstämmer delvis med regeringens. Utredningen föreslår även en ändamålsbestämmelse för behandling av personuppgifter vid begäran om information av enskilda eller vid tillsyn.

Remissinstanserna: *Försvarets radioanstalt* välkomnar utredningens förslag om ett särskilt ändamål för behandling av personuppgifter vid begäran om information av enskilda eller vid tillsyn. *Datainspektionen* anser att det inte är nödvändigt att i de nya lagarna ange att Försvarsmakten och Försvarets radioanstalt ska kunna behandla personuppgifter för att kunna tillgodose enskildas behov av information och för att kunna lämna information vid tillsyn och kontroll.

Skälen för regeringens förslag

Behandling ska få ske för vetenskapliga, statistiska eller historiska ändamål

Möjligheten att bevara personuppgifter som behandlas automatiserat för vetenskapliga, statistiska eller historiska ändamål är enligt FM-PuL och FRA-PuL kopplad till regler om gallring. Enligt lagarna 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 (6 kap. 1 §). Riksarkivet har rätt att besluta om bevarande. Ett sådant beslut får till följd att uppgifterna inte gallras (12 § FM-PuF och FRA-PuF).

Regeringen konstaterar att vikten av att kunna behandla personuppgifter för vetenskapliga, statistiska eller historiska syften gör sig gällande även för den verksamhet som regleras i de nya lagarna. Som utredningen föreslår bör det i de nya lagarna därför anges att personuppgifter får behandlas för vetenskapliga, statistiska och historiska ändamål.

Enligt utredningen och *Försvarets radioanstalt* bör det i de nya lagarna även införas 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. Som *Datainspektionen* uppmärksammar saknar utredningens förslag motsvarighet i annan dataskyddslagstiftning och behovet av en sådan bestämmelse kan ifrågasättas. De aktuella situationerna medför en nödvändig behandling av personuppgifter, på motsvarande sätt som vid myndigheternas planering, uppföljning och utvärdering av verksamheten, dvs. behandling som får ske utan att det finns behov av en särskild ändamålsbestämmelse (se Tullverkets brottsbekämpning – Effektivare uppgiftsbehandling, prop. 2004/05:164 s. 179 och Åklagardatalag, prop. 2014/15:63 s. 63).

Regeringen anser att utredningens förslag i denna del inte bör genomföras.

7.6 Behandling av uppgifter om lagöverträdelser

Regeringens förslag: Försvarsmakten får behandla personuppgifter som rör lagöverträdelser om det är nödvändigt för myndighetens verksamhet.

Utredningen lämnar inte något förslag i denna del.

Remissinstanserna: *Försvarsmakten* anför att myndigheten i sin verksamhet har behov av att behandla personuppgifter som rör lagöverträdelser.

Skälen för regeringens förslag: Myndigheter får enligt dataskyddslagen behandla uppgifter om lagöverträdelser (3 kap. 8 §). Motsvarande reglering fanns tidigare i den numera upphävda personuppgiftslagen (21 §).

Försvarsmakten behandlar för närvarande personuppgifter som rör lagöverträdelser inom ramen för exempelvis militär säkerhetstjänst vilket framgår av de tillåtna ändamålen för personuppgiftsbehandling (1 kap. 10 § FM-PuL). Att uppgifter rörande lagöverträdelser kommer att behandlas även framöver framgår av de föreslagna ändamålen för personuppgiftsbehandling för militär säkerhetstjänst (se avsnitt 7.2.3). Ändamålen omfattar exempelvis kartläggning av verksamhet som kan innefatta brott samt uppgifter som framkommit inom ramen för säkerhetsprövning enligt säkerhetsskyddslagen. I en säkerhetsprövning görs en registerkontroll, vilket innebär att uppgifter som rör lagöverträdelser behandlas avseende de individer som får utfall i registerkontrollen. Misstankar om brott som Försvarsmakten behandlar inom ramen för dessa ändamål utgör uppgifter om lagöverträdelser (prop. 2017/18:105 s. 98–99).

Försvarsmakten kan även inom ramen för sin personaladministrativa verksamhet behöva behandla personuppgifter som rör lagöverträdelser. Som *Försvarsmakten* anför bör den nya lagen därför innehålla en bestämmelse som innebär att Försvarsmakten får behandla person-

uppgifter som rör lagöverträdelser om det är nödvändigt för myndighetens verksamhet. Regeringen föreslår att lagtexten utformas i enlighet med detta.

8 Behandlingen av personuppgifter

8.1 Personuppgifter ska behandlas enligt vissa villkor

8.1.1 Personuppgifter ska behandlas författningsenligt och på ett korrekt sätt

Regeringens förslag: Personuppgifter ska behandlas författningsenligt och på ett korrekt sätt.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Ingen remissinstans invänder mot utredningens förslag.

Skälen för regeringens förslag: Försvarsmakten respektive Försvarets radioanstalt ska enligt nuvarande ordning se till att personuppgifter behandlas bara om det är lagligt och att personuppgifter alltid behandlas på ett korrekt sätt och i enlighet med god sed (1 kap. 6 § 1 och 2 FM-PuL och FRA-PuL, jfr 1 kap. 9 § RF och 5 § förvaltningslagen [2017:900]). Som utredningen föreslår bör detta, med vissa språkliga justeringar, komma till uttryck även i de nya lagarna.

8.1.2 Personuppgifter ska vara riktiga, adekvata och relevanta

Regeringens förslag: De personuppgifter som behandlas ska vara riktiga och, om det är nödvändigt, uppdaterade. Personuppgifter som behandlas ska vara adekvata och relevanta i förhållande till ändamålen med behandlingen.

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.

Utredningens förslag överensstämmer i sak med regeringens.

Remissinstanserna: Ingen remissinstans invänder mot utredningens förslag.

Skälen för regeringens förslag

Personuppgifter ska vara riktiga och – om nödvändigt – uppdaterade

Enligt gällande rätt ska Försvarsmakten respektive Försvarets radioanstalt se till att de personuppgifter som behandlas är riktiga och, om det är

nödvändigt, aktuella (1 kap. 6 § 7 FM-PuL och FRA-PuL). Detta bör, som utredningen föreslår, gälla även fortsättningsvis. I linje med annan dataskyddslagstiftning bör ordet aktuella ersättas med uppdaterade.

En uppgift är riktig om den stämmer överens med de verkliga förhållandena. För att bestämma vilka verkliga förhållanden som personuppgifterna ska spegla får ledning sökas i ändamålen med behandlingen. Bedömningen av om en personuppgift är riktig ska emellertid inte utgå från enbart ändamålen med behandlingen. Att uppgifter som förekommer bl.a. i försvarsunderrättelseverksamheten har en särskild karaktär måste också beaktas. Frågan om en uppgift är riktig måste därför även ses mot bakgrund av vad uppgiften rör, när den lämnas och vem som lämnar den.

Kravet på att de behandlade uppgifterna ska vara uppdaterade bör enbart gälla om det är nödvändigt. Frågan om det är nödvändigt att uppgifterna är uppdaterade får avgöras med hänsyn till ändamålen med behandlingen. Ett tänkbart exempel kan vara adressuppgifter som ändras under handläggningen av ett ärende och därmed behöver uppdateras. Som utredningen föreslår bör de nya lagarna innehålla bestämmelser om detta.

Uppgifter som beskriver en persons utseende ska utformas på ett objektivt sätt

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). Regeringen anser i likhet med utredningen att motsvarande innehåll bör tas in i de nya lagarna.

Personuppgifter ska vara adekvata och relevanta

Försvarsmakten respektive Försvarets radioanstalt ska enligt nuvarande ordning se till att de personuppgifter som behandlas är adekvata och relevanta i förhållande till ändamålen med behandlingen och att inte fler personuppgifter behandlas än vad som är nödvändigt med hänsyn till ändamålen med behandlingen (1 kap. 6 § 5 och 6 FM-PuL och FRA-PuL). Att personuppgifter ska vara adekvata och relevanta innebär bl.a. att ovidkommande personuppgifter inte får behandlas. Vilka uppgifter som är adekvata och relevanta måste enligt regeringens mening bedömas i förhållande till ändamålen med behandlingen. Detsamma gäller hur många personuppgifter det finns behov av att behandla.

Som utredningen föreslår bör motsvarande bestämmelser föras in i de nya lagarna.

8.2 Behandling av känsliga personuppgifter

Regeringens 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. Om personuppgifter behandlas får de dock kompletteras med sådana uppgifter när det är absolut nödvändigt för ändamålen med behandlingen.

Biometriska uppgifter får behandlas om det är absolut nödvändigt för ändamålen med 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 ändamålen med behandlingen. Detsamma gäller biometriska uppgifter.

Utredningens förslag överensstämmer i sak med regeringens.

Remissinstanserna: *Datainspektionen* anser att sökförbudet avseende känsliga personuppgifter bör utformas enligt samma modell som har föreslagits i fråga om Säkerhetspolisen (SOU 2017:74). Enligt Datainspektionen bör det även övervägas om sökningar på känsliga personuppgifter bör dokumenteras särskilt.

Skälen för regeringens förslag

Uppgifter om ras, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, hälsa eller sexualliv

Uppgifter om en persons ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexualliv får enligt gällande rätt behandlas endast som 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 (1 kap. 12 § FM-PuL och 1 kap. 11 § FRA-PuL).

I samband med tillkomsten av FM-PuL och FRA-PuL framhölls i förarbetena till lagarna att Försvarsmakten och Försvarets radioanstalt många gånger har ett befogat intresse av att kunna registrera och på annat sätt behandla känsliga personuppgifter i de verksamheter som omfattas av förslagen. Det kan t.ex. vara nödvändigt inom ramen för Sveriges deltagande i internationella fredsbevarande och humanitära insatser. I dessa uppdrag ingår ofta att skydda en viss minoritet. För att de svenska enheterna inom en sådan mission ska kunna utföra sina uppgifter kan det därför vara nödvändigt att uppgifter behandlas rörande t.ex. etnisk härkomst eller religiös övertygelse. Här bidrar såväl den militära underrättelse- och säkerhetstjänsten som Försvarets radioanstalt med underrättelser. Även i övrigt finns det ett behov av att kunna behandla känsliga personuppgifter. Ofta är just det faktum att en person tillhör ett politiskt parti eller annan organisation av grundläggande betydelse från

försvarsunderrättelse- eller säkerhetstjänstsynpunkt. En sådan omständighet får dock aldrig utgöra ensam grund för behandlingen. Det ligger således i verksamhetens natur att denna typ av uppgifter kan ha en betydelse för resultatet av den slutliga analysen (prop. 2006/07:46 s. 74–75).

I den verksamhet som omfattas av detta lagstiftningsärende är fortsatt uppgifter om etniskt ursprung, politiska åsikter och religiös övertygelse sådana faktorer som är av stor betydelse när det gäller att bedöma personers eller gruppers agerande i ett ur försvarsunderrättelseperspektiv relevant avseende. Allmänt gäller att stor försiktighet måste iakttas vid all behandling av känsliga personuppgifter. Regeringen anser, i likhet med utredningen, att det i de nya lagarna därför bör anges att sådan behandling endast får äga rum då det är absolut nödvändigt för verksamheten. Detta för att markera att denna möjlighet ska användas mycket restriktivt. Försvarsmakten respektive Försvarets radioanstalt bör vidare, på samma sätt som hittills, få behandla känsliga personuppgifter om en person endast om uppgifterna kompletterar personuppgifter som behandlas på annan grund.

Biometriska och genetiska uppgifter

Med biometriska uppgifter avses enligt förslaget personuppgifter som rör en fysisk persons fysiska, fysiologiska eller beteendemässiga kännetecken som tagits fram genom särskild teknisk behandling och som möjliggör eller bekräftar identifiering av personen i fråga (se avsnitt 6.5). Försvarsmakten och Försvarets radioanstalt behandlar biometriska uppgifter i sina försvarsunderrättelseverksamheter, och Försvarsmakten behandlar även sådana uppgifter inom ramen för den militära säkerhetstjänsten. 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.

Bestämmelsen om att känsliga personuppgifter endast får behandlas såsom komplement till personuppgifter som behandlas på annan grund är inte tillämplig när det gäller biometriska personuppgifter, t.ex. oidentifierade avtryck eller spår. Som utredningen anför finns det 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 ändamålen med behandlingen.

Med genetiska uppgifter avses personuppgifter som rör en persons nedärvda eller förvärvade genetiska kännetecken och som framför allt härrör från analys av ett spår av eller ett biologiskt prov från personen i fråga (se avsnitt 6.5). Det innebär att ett dna-spår eller ett dna-prov som sådant inte utgör genetiska uppgifter, utan det är enbart den information som kan tas fram ur spåret eller provet som utgör sådana uppgifter (prop. 2018/19:163 s. 77).

Regeringen anser att genetiska uppgifter är av synnerligen integritetskänslig natur. Som utredningen föreslår bör det av de nya lagarna uttryckligen framgå att behandling av genetiska uppgifter inte är tillåten.

Uppgifter om sexuell läggning

Enligt FM-PuL och FRA-PuL är uppgifter om fysiska personers sexualliv känsliga personuppgifter. Uppgifter om sexuell läggning har i rättstillämpningen också ansetts omfattas av nuvarande bestämmelser. I enlighet med utredningens förslag bör den nya regleringen uttryckligen omfatta även uppgifter om sexuell läggning.

Sökning av känsliga personuppgifter får endast ske om det är absolut nödvändigt för verksamheten

Försvarsmaktens och Försvarets radioanstalts verksamheter förutsätter, som anges ovan, att sökning i viss utsträckning kan ske även avseende känsliga personuppgifter. Sådan behandling behöver då regleras särskilt. *Datainspektionen* framhåller att sökförbudet avseende känsliga personuppgifter bör utformas som ett generellt förbud med utgångspunkt från syftet med sökningen och med undantag anpassade för Försvarsmaktens och Försvarets radioanstalts verksamheter. Dessutom bör det enligt Datainspektionen övervägas om sökningar på känsliga personuppgifter bör dokumenteras särskilt.

Regeringen konstaterar att automatiserad behandling av personuppgifter, i synnerhet i samlingar av uppgifter, ger stora möjligheter att söka och sammanställa information. Dessa möjligheter innebär särskilt stora risker för intrång i den personliga integriteten. I syfte att minska denna risk finns det anledning att överväga att införa en begränsning av sökmöjligheterna. Samtidigt måste beaktas att möjligheten att enkelt och snabbt söka information skapar förutsättningar för en rationell verksamhet. En eventuell begränsning bör därför enligt regeringens mening inte utformas så snävt att den medför onödiga effektivitetsförluster ur ett verksamhetsperspektiv.

Behovet av en reglering som begränsar vilka uppgifter som ska få användas vid sökning gör sig framförallt gällande i fråga om känsliga personuppgifter. I konsekvens med de grundläggande kraven för behandling av känsliga personuppgifter bör sökning efter information om känsliga personuppgifter endast få ske om det är absolut nödvändigt för syftet med behandlingen. Det innebär att en uppgift om t.ex. etnisk härkomst bör få användas som sökbegrepp bara under den förutsättningen att det är absolut nödvändigt för att få fram den information som behövs för att t.ex. utföra en fredsbevarande eller humanitär insats som åligger svenskt förband eller annan organisationsenhet. Bestämmelsen om behandling av känsliga personuppgifter och sökning med sådana uppgifter bör vara generell, dvs. den bör gälla såväl för behandling i Försvarsmaktens och Försvarets radioanstalts olika gemensamt tillgängliga uppgiftssamlingar som för annan behandling. Detta gäller enligt nuvarande ordning och bör enligt regeringens uppfattning gälla även fortsättningsvis.

Denna ordning innebär att sökning av känsliga personuppgifter är föremål för en mycket strikt prövning i myndigheternas verksamheter, där

absolut nödvändighet är en grundförutsättning för sådana sökningar. Skyddet för den enskildes integritet ges på så sätt ett starkt och nödvändigt skydd. Regeringen anser att detta utgör en väl avvägd balans mellan verksamhetens krav och integritetsskyddet för enskilda. Någon justering i förhållande till utredningens förslag bör därför inte göras.

8.3 Behandling av personnummer och samordningsnummer

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

Utredningens förslag överensstämmer delvis med regeringens förslag. Utredningen föreslår inte att regleringen ska gälla för Försvarets radioanstalt.

Remissinstanserna: *Försvarets radioanstalt* instämmer i utredningens bedömning att myndigheten i liten omfattning behandlar personnummer och samordningsnummer. *Datainspektionen* ifrågasätter utredningens ställningstagande i fråga om Försvarets radioanstalt.

Skälen för regeringens förslag: Enligt nuvarande reglering får uppgifter om personnummer eller samordningsnummer bara behandlas när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering, eller något annat beaktansvärt skäl (1 kap. 13 § FM-PuL och 1 kap. 12 § FRA-PuL).

Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst respektive Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet grundas inte på samtycke från den enskilde. Försvarsunderrättelseverksamheten är inriktad på utländska förhållanden och det är inte vanligt förekommande att personnummer och samordningsnummer behandlas inom denna verksamhet. Detsamma gäller i fråga om Försvarets radioanstalts informationssäkerhetsverksamhet.

För Försvarsmaktens verksamhet innebär den nya lagen ett utökat tillämpningsområde i förhållande till FM-PuL, vilket medför att myndigheten kommer att behandla personnummer och samordningsnummer i stor utsträckning, bl.a. när det gäller egen personal. En bestämmelse som motsvarar nuvarande ordning bör, som utredningen föreslår, införas i den nya lagen om behandling av personuppgifter vid Försvarsmakten.

Utredningen föreslår inte någon bestämmelse om behandling av personnummer och samordningsnummer för Försvarets radioanstalt. Till skillnad från utredningen och *Försvarets radioanstalt* anser regeringen dock inte att det faktum att Försvarets radioanstalt i endast begränsad utsträckning behandlar personnummer och samordningsnummer innebär att det saknas skäl att reglera detta. I den mån sådan behandling aktualiseras bör motsvarande regelverk gälla även för Försvarets radioanstalt. Regeringen föreslår att en sådan bestämmelse införs i den nya lagen om behandling av personuppgifter vid Försvarets radioanstalt.

8.4 Behandling av offentliggjorda personuppgifter

Regeringens förslag: Försvarsmakten får behandla andra känsliga personuppgifter än genetiska uppgifter samt personnummer och samordningsnummer, om den registrerade har lämnat sitt uttryckliga samtycke till behandlingen eller har offentliggjort personuppgifterna på ett tydligt sätt.

Försvarets radioanstalt får behandla andra känsliga personuppgifter än genetiska uppgifter samt personnummer och samordningsnummer, om den registrerade har offentliggjort personuppgifterna på ett tydligt sätt.

Utredningens förslag överensstämmer i huvudsak med regeringens.

Remissinstanserna yttrar sig inte särskilt över utredningens förslag.

Skälen för regeringens förslag: FM-PuL och FRA-PuL saknar bestämmelser om att bl.a. känsliga personuppgifter får behandlas, om den registrerade har lämnat sitt uttryckliga samtycke till behandlingen eller på ett tydligt sätt har offentliggjort uppgifterna. Som utredningen föreslår bör en sådan reglering, med undantag för genetiska uppgifter, på ett för Försvarsmakten och Försvarets radioanstalt anpassat sätt införas i de nya lagarna.

I Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet och informationssäkerhetsverksamhet och Försvarsmaktens försvarsunderrättelseverksamhet aktualiseras inte några samtyckessituationer. Sådana situationer kan emellertid förekomma i Försvarsmaktens övriga verksamhet, exempelvis i Försvarsmaktens militära säkerhetstjänst vid säkerhetsprövningar. Regeringen föreslår, i likhet med utredningen, att Försvarsmakten ska få behandla andra känsliga personuppgifter än genetiska uppgifter samt personnummer och samordningsnummer, om den registrerade har lämnat sitt uttryckliga samtycke till behandlingen.

I enlighet med utredningens förslag bör Försvarsmakten och Försvarets radioanstalt också få behandla andra känsliga personuppgifter än genetiska uppgifter samt personnummer och samordningsnummer, om den registrerade på ett tydligt sätt har offentliggjort uppgifterna. Ett tydligt offentliggörande kan ske t.ex. genom att den registrerade gör uppgifterna tillgängliga på internet. Enligt utredningens förslag får enbart Försvarsmakten behandla personnummer och samordningsnummer i en sådan situation. Regeringen anser inte att denna skillnad är sakligt motiverad och föreslår därför att detsamma även ska gälla för Försvarets radioanstalt.

8.5 Behandling av personuppgifter i vissa fall

Regeringens förslag: Försvarets radioanstalts och Försvarsmaktens hantering av information som innebär behandling av personuppgifter ska inte anses oförenlig med bestämmelserna om tillåtlighet, grundläggande krav, känsliga personuppgifter, personnummer och samordningsnummer, i det skede av behandlingen då det ännu inte har kunnat fastställas vilka personuppgifter som informationen innehåller.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: *Försvarets radioanstalt* framhåller att frågan är av central betydelse för myndighetens verksamhet. *Datainspektionen* anser att en anpassning i förhållande till nuvarande ordning är befogad. Myndigheten ifrågasätter dock utredningens förslag att regleringen även ska omfatta Försvarets radioanstalts informationssäkerhetsverksamhet och Försvarsmakten.

Skälen för regeringens förslag

Försvarets radioanstalt

Enligt nuvarande ordning ska 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 anses som oförenlig med bestämmelserna om grundläggande krav, ändamål samt behandling av känsliga personuppgifter och personnummer (1 kap. 13 § FRA-PuL). 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 bestämmelserna om detta.

Försvarets radioanstalts inhämtning av signaler i tråd ska enligt lagen om signalspaning i försvarsunderrättelseverksamhet ske automatiserat och får endast avse signaler som identifierats genom sökbegrepp. Även vid annan inhämtning ska sökbegrepp användas för identifieringen av signaler (3 §). Detta förfarande reducerar informationsmängden på ett ändamålsenligt sätt före själva inhämtningen och tillvaratar därmed också integritetsskyddsintresset. Behandling av personuppgifter omfattar all slags behandling, alltså även sådan som sker på automatisk väg (1 kap. 4 §). 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. Det är därmed ingen analytiker som i detta skede bearbetar och bedömer uppgifterna på ett sådant sätt att det går att avgöra om bestämmelserna i FRA-PuL om grundläggande krav, ändamål, känsliga personuppgifter samt personnummer och samordningsnummer aktualiseras.

I rättstillämpningen har uppkommit fråga 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 om bl.a. grundläggande krav i FRA-PuL. Utredningen konstaterar att bestämmelsen i 1 kap. 13 § FRA-PuL står i konflikt med den personuppgiftsbehandling som lagen om signalspaning i försvarsunderrättelseverksamhet förutsätter ska ske med automatik hos Försvarets radioanstalt efter inhämtningsskedet (Behandlingen av personuppgifter vid Försvarsmakten och Försvarets radioanstalt, SOU 2018:63 s. 194). Datainspektionen har gjort motsvarande bedömning i ett tillsynsbeslut den 24 oktober 2016 (dnr 2331-2015). Som utredningen föreslår bör den nya regleringen därför utformas så att den tar sikte på det skede då det inte har kunnat fastställas vilka personuppgifterna är.

Även i Försvarets radioanstalts informationssäkerhetsverksamhet kan det förekomma automatiserade skeenden som inledningsvis innebär att eventuella personuppgifter då ännu inte finns tillgängliga för bedömning i verksamheten, eftersom det också där kan krävas kryptoforcering innan uppgifterna finns tillgängliga för bedömning. Till skillnad från Datainspektionen anser regeringen, i likhet med utredningen, att bestämmelsen därför bör omfatta även Försvarets radioanstalts informationssäkerhetsverksamhet. Enligt den föreslagna bestämmelsen ska således Försvarets radioanstalts hantering av information som innebär behandling av personuppgifter inte anses oförenlig med bestämmelserna om tillåtlighet, grundläggande krav, känsliga personuppgifter samt personnummer och samordningsnummer i det skede av behandlingen då det ännu inte har kunnat fastställas vilka personuppgifter som informationen innehåller.

Försvarsmakten

För Försvarsmakten finns för närvarande inte någon motsvarighet till regleringen om behandling av personuppgifter i vissa fall. Enligt utredningens förslag ska den nya regleringen även gälla för Försvarsmakten, vilket *Datainspektionen* ifrågasätter.

Regeringen konstaterar att syftet med förslaget är att kunna omhänderta den särskilda situationen att inhämtade uppgifter kräver kryptoforcering eller en översättning innan det står klart om det är fråga om personuppgifter som behandlas, eller om en automatiserad hantering av uppgifterna medför att en sådan manuell bedömning inte kan göras omedelbart. Sådana situationer kan även uppkomma i Försvarsmaktens verksamhet, t.ex. när myndigheten mottar information från andra myndigheter.

Lagrådet ifrågasätter om bestämmelserna om undantag som föreslås i de nya lagarna ska vara fullt ut tillämpliga också i de fall när man vet att materialet innehåller personuppgifter och osäkerheten endast gäller vilka personuppgifter det är fråga om. Enligt Lagrådet är det även sannolikt att undantaget genom uppräkningen av paragrafer har blivit för omfattande.

Det bör understrykas att förslaget avser att fånga in särskilda och avgränsade situationer, nämligen behandling av personuppgifter i ett skede där det ännu inte har kunnat fastställas vilka personuppgifter som informationen innehåller, t.ex. på grund av att informationen är krypterad eller att personuppgifter som behandlas automatiskt inte blir föremål för manuell granskning. Behandling av personuppgifter enligt förslaget avser även insamling av sådana uppgifter. Regeringen anser att det därför är viktigt att regleringen uttryckligen slår fast att en hantering av information som innebär behandling av personuppgifter inte ska anses vara oförenligt med vissa grundläggande bestämmelser i de nya lagarna i det skede av behandlingen då det inte har kunnat fastställas vilka personuppgifter som informationen innehåller. Det finns inte skäl att göra någon åtskillnad i sak mellan Försvarsmakten och Försvarets radioanstalt i fråga om vilka bestämmelser som undantaget bör avse. I förhållande till lagrådsremissen bör därför lagförslaget avseende Försvarsmakten justeras på så sätt att det även omfattar personuppgifter som utgör allmänt tillgänglig information (jfr. avsnitt 7.4).

8.6 Längsta tid som personuppgifter får behandlas

Regeringens förslag: Personuppgifter får inte behandlas under längre tid än vad som behövs för ändamålet med behandlingen.

Utredningens förslag överensstämmer delvis med regeringens. Utredningens förslag avser endast personuppgifter som behandlas automatiserat.

Remissinstanserna: *Försvarsmakten* anser inte att det bör göras en avgränsning till enbart personuppgifter som behandlas automatiserat. Enligt *Datainspektionen* bör de nya lagarna innehålla särskilda regler om att vissa personuppgifter ska rensas efter vissa angivna tidpunkter. Datainspektionen anser även att utredningens förslag om att bevara uppgifter för historiska, statistiska och vetenskapliga ändamål är alltför långtgående. *Riksarkivet* anser att det är viktigt att det finns möjlighet att bevara uppgifter inom underrättelseverksamheten. Enligt *Statens inspektion för försvarsunderrättelseverksamheten* kan det finnas skäl att överväga någon form av särskild reglering av längsta tid för behandling för vissa av de föreslagna ändamålsbestämmelserna.

Skälen för regeringens förslag: Hur länge personuppgifter får bevaras enligt FM-PuL och FRA-PuL regleras i lagarnas bestämmelser om gallring (6 kap. 1 §). Personuppgifter som behandlas automatiserat ska enligt bestämmelserna 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. Som *Datainspektionen* uppmärksammar har regeringen i förordningar i vissa fall bestämt uttryckliga tidsgränser för när gallring av personuppgifter i angivna uppgiftssamlingar senast ska ske.

I försvarsunderrättelseverksamheten och den militära säkerhetstjänsten behöver personuppgifter inte sällan behandlas under mycket lång tid. Enligt nuvarande huvudregel ska personuppgifter gallras när de inte längre behövs för det ändamål för vilket de behandlas. Det ska ske en fortlöpande prövning om en personuppgift ska behandlas eller inte. Som utredningen föreslår bör detta gälla även fortsättningsvis. Regeringen kommer också även fortsättningsvis att i förordning kunna meddela föreskrifter som innebär avsteg från huvudregeln att personuppgifter ska rensas ur verksamhetssystemen när de inte längre behövs för det ändamål för vilket de behandlas.

Regeringen anser, i likhet med *Försvarsmakten,* att de nya bestämmelserna bör utformas så att de följer den definition som föreslås för behandling av personuppgifter och som innebär att behandling kan ske såväl automatiserat som manuellt (jfr avsnitt 6.5).

Statens inspektion för försvarsunderrättelseverksamheten lyfter frågan om lagarna bör innehålla särskilda bestämmelser om längsta tid för behandling av personuppgifter som är allmänt tillgängliga (jfr avsnitt 7.4) och personuppgifter i vissa fall (jfr avsnitt 8.5). Regeringen bedömer dock att det inte är nödvändigt. Regeringen anser därför att en sådan särskild bestämmelse om längsta tid för nu aktuella behandling inte bör införas i de nya lagarna. I enlighet med utredningens förslag kan emellertid

regeringen, eller den myndighet som regeringen bestämmer, meddela föreskrifter eller beslut i ett enskilt fall om att personuppgifter får behandlas under endast viss tid. En sådan ordning gäller enligt nuvarande ordning och bör lämpligen gälla även enligt de nya lagarna.

I de nya lagarna bör det även föras in upplysningsbestämmelser om att regeringen, eller den myndighet som regeringen bestämmer, kan meddela föreskrifter eller beslut i ett enskilt fall om att personuppgifter får fortsätta behandlas för arkivändamål av allmänt intresse eller för vetenskapliga, statistiska eller historiska ändamål. Förslaget påverkar inte Försvarsmaktens och Försvarets radioanstalts möjligheter att arkivera och bevara allmänna handlingar, eller att lämna arkivmaterial till en arkivmyndighet.

9 Gemensamt tillgängliga personuppgifter

Regeringens förslag: Personuppgifter får göras gemensamt tillgängliga vid Försvarsmakten om det behövs för något av de ändamål för vilka myndigheten får behandla personuppgifter.

Personuppgifter som görs gemensamt tillgängliga inom Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst ska även fortsättningsvis behandlas i uppgiftssamlingar.

Personuppgifter får göras gemensamt tillgängliga vid Försvarets radioanstalt och behandlas i uppgiftssamlingar om det behövs för de ändamål som anges i den nya lagen.

Utredningens förslag överensstämmer i huvudsak med regeringens.

Remissinstanserna: *Försvarsmakten* anser att utredningens lagförslag bör gälla generellt för myndigheten. Myndigheten förordar vidare att uppgiftssamlingar endast ska användas för gemensamt tillgängliga uppgifter i myndighetens försvarsunderrättelseverksamhet och militära säkerhetstjänst. Övriga remissinstanser yttrar sig inte särskilt över utredningens förslag.

Skälen för regeringens förslag

Nuvarande reglering om gemensamt tillgängliga uppgifter

Enligt FM-PuL och FRA-PuL är en uppgiftssamling en samling med uppgifter som med hjälp av automatiserad behandling används gemensamt (1 kap. 4 §). Personuppgifter får, under de förutsättningar som anges i lagarna, behandlas i uppgiftssamlingar för Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst samt för Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet. Regeringen kan också meddela föreskrifter eller beslut i enskilda fall om vilka uppgiftssamlingar som får finnas och vilka uppgifter som får behandlas i respektive samling (1 kap. 7 § FM-PuL och FRA-PuL).

Ordet uppgiftssamling är avsett att vara teknikneutralt. Avgörande för när automatiserat behandlade uppgifter ska anses ingå i en uppgiftssamling är 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 typiskt sett åtkomlig endast för handläggaren själv och systemadministratören vid myndigheten. En sådan uppgift bör 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.

En tydligare reglering för gemensamt tillgängliga uppgifter och direktåtkomst

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 är inte att anse som gemensamt tillgängliga.

Försvarsmakten invänder mot utredningens förslag att införa särskilda bestämmelser om gemensamt tillgängliga uppgifter och hänvisar till betänkandet SOU 2017:97 Totalförsvarsdatalag – Rekryteringsmyndighetens personuppgiftsbehandling. Regeringen anser inte att jämförelsen med totalförsvarsdatalagen är relevant då den lagen är avgränsad till behandlingen av personuppgifter om totalförsvarspliktiga och annan personal som har en uppgift inom totalförsvaret vid höjd beredskap.

Uppgiftssamlingar används för närvarande i FM-PuL och FRA-PuL som beteckning för gemensamt tillgängliga uppgifter. Utredningen föreslår att ordet även ska användas i de nya lagarna, men för Försvarsmakten endast i fråga om försvarsunderrättelseverksamheten och den militära säkerhetstjänsten. Enligt utredningen fyller ordet uppgiftssamling även fortsatt en funktion i regleringen om behandlingen av personuppgifter i dessa verksamheter. Regeringen, som instämmer i detta, anser att utredningens förslag att de nya lagarna ska innehålla särskilda bestämmelser om gemensamt tillgängliga uppgifter bör genomföras.

Försvarsmakten och Försvarets radioanstalt förutsätts kunna samarbeta med andra, företrädesvis myndigheter. Inom ramen för sådant samarbete kan personuppgifter i gemensamma projekt komma att behandlas. För att bl.a. möjliggöra ett sådant samarbete gör regeringen bedömningen att vissa myndigheter bör kunna medges direktåtkomst till uppgifter som har gjorts gemensamt tillgängliga inom Försvarsmakten och Försvarets radioanstalt (jfr avsnitt 10.3.1). 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.

På samma sätt som enligt nuvarande ordning är det inte möjligt att i författning ange någon exakt gräns för när en viss behandling ska anses ske i en uppgiftssamling och därmed omfattas av de bestämmelser som

reglerar sådana samlingar. Myndigheterna måste i det enskilda fallet avgöra om uppgifter som behandlas automatiserat är gemensamt tillgängliga eller inte. En handläggare inom Försvarsmakten eller Försvarets radioanstalt bör enligt regeringen 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 onödig detaljreglering i lag bör därför regeringen, eller den myndighet som regeringen bestämmer, även fortsättningsvis kunna meddela närmare föreskrifter eller beslut i enskilda fall om vilka uppgiftssamlingar som får finnas och vilka personuppgifter som får behandlas i respektive samling. Regeringen föreslår att en upplysningsbestämmelse om detta förs in i de nya lagarna.

Enligt förslaget till ny lag för Försvarets radioanstalt ska personuppgifter få göras gemensamt tillgängliga och behandlas i uppgiftssamlingar under vissa förutsättningar. *Lagrådet* anser att förslaget enligt sin lydelse förutsätter att det även ska få finnas gemensamt tillgängliga uppgifter som inte är en uppgiftssamling. Regeringen delar inte Lagrådets tolkning av förslaget. Försvarets radioanstalts behandling av gemensamt tillgängliga uppgifter kommer endast att ske i uppgiftssamlingar och regeringen bedömer att förslaget är ändamålsenligt.

Som *Lagrådet* uppmärksammar är det väsentligt att uttrycket gemensamt tillgängliga uppgifter genomgående ges samma innebörd i de nya lagarna. Regeringen ser dock inte något behov av att införa särskilda definitionsbestämmelser för att säkerställa detta.

Närmare om Försvarsmaktens behandling av gemensamt tillgängliga uppgifter

När det gäller Försvarsmaktens behandling av gemensamt tillgängliga uppgifter i annan verksamhet än försvarsunderrättelseverksamhet och militär säkerhetstjänst ser utredningen, med hänvisning till bl.a. befintliga användningsbegränsningar för myndighetens personal, inte behov av att uppställa krav på särskilda uppgiftssamlingar. Utredningen föreslår dock att Försvarsmakten ska få bestämma vilka uppgiftssamlingar som ska införas vid myndigheten när det gäller behandling av personuppgifter utanför försvarsunderrättelseverksamheten och den militära säkerhetstjänsten.

Regeringen instämmer i *Försvarsmaktens* uppfattning att uppgiftssamlingar endast ska användas inom de verksamheter som gäller enligt nuvarande lagstiftning för Försvarsmakten. Personuppgiftslagen, som för närvarande gäller för sådan behandling av personuppgifter för övrig verksamhet hos Försvarsmakten där den nya lagen ska tillämpas,

innehåller inte något krav på uppgiftssamlingar. Detsamma gäller för EU:s dataskyddsförordning och dataskyddslagen. Det regelverk för behandlingen av personuppgifter som den nya lagen i övrigt innehåller ger enligt regeringen ett fullgott skydd för enskildas integritet. Mot denna bakgrund saknas skäl att införa en ordning som innebär ett obligatoriskt krav på uppgiftssamlingar för den uppgiftsbehandling som sker utanför Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst.

10 Informationsutbyte

10.1 Olika former av elektroniskt utlämnande

Utlämnande på medium för automatiserad behandling

I princip anses allt elektroniskt utlämnande som inte görs genom direktåtkomst utlämnat på medium för automatiserad behandling. Högsta förvaltningsdomstolen har ansett att gränsdragningen mellan vad som är direktåtkomst och annat utlämnande på medium för automatiserad behandling beror på om den aktuella uppgiften kan anses förvarad hos den mottagande myndigheten enligt 2 kap. 3 § andra stycket tryckfrihetsförordningen (HFD 2015 ref. 61).

Utlämnande på medium för automatiserad behandling 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.

Direktåtkomst

Det finns inte någon legaldefinition av ordet direktåtkomst. Det som typiskt sett avses är att någon har direkt tillgång till någon annans register eller databas och på egen hand kan söka efter information, dock utan att kunna påverka innehållet i registret eller databasen. Enligt Informationshanteringsutredningen bör direktåtkomst anses föreligga om en myndighet hos en annan myndighet har sådan teknisk tillgång till upptagningar som avses i 2 kap. 3 § andra stycket tryckfrihetsförordningen, dvs. om upptagningen är tillgänglig för myndigheten med tekniskt hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas, avlyssnas eller på annat sätt uppfattas (Myndighetsdatalag, SOU 2015:39 s. 390–393). Högsta förvaltningsdomstolen har använt samma definition av direktåtkomst (HFD 2015 ref. 61). I begreppet direktåtkomst ligger också att den som är personuppgiftsansvarig för registret eller databasen saknar kontroll över vilka uppgifter som den som har direktåtkomst vid ett

visst tillfälle tar del av. Från integritetssynpunkt har det därför ansetts viktigt att frågor om tillgång till uppgifter genom direktåtkomst regleras särskilt i registerlagstiftningarna (Ökat informationsutbyte mellan arbetslöshetsförsäkringen, socialförsäkringen och studiestödet, prop. 2000/01:129 s. 74, Lag om behandling av personuppgifter i den arbetsmarknadspolitiska verksamheten, prop. 2001/02:144 s. 35–39 och Elektronisk informationsöverföring hos arbetslöshetskassorna och inom Arbetsmarknadsverket, prop. 2005/06:52 s. 8).

Vid direktåtkomst fattas beslut om överföring i varje enskilt fall av mottagaren. Den faktiska begränsningen av direktåtkomsten görs med hjälp av olika tekniska lösningar, beroende på hur omfattningen av direktåtkomsten har begränsats i det enskilda fallet.

10.2 Elektronisk informationsöverföring på annat sätt än direktåtkomst

Regeringens förslag: Försvarsmakten ska få lämna ut personuppgifter elektroniskt på annat sätt än genom direktåtkomst, om det inte är olämpligt. Regeringen kan meddela föreskrifter som begränsar denna möjlighet.

Försvarets radioanstalt ska få lämna ut personuppgifter elektroniskt på annat sätt än genom direktåtkomst, om regeringen har meddelat föreskrifter eller beslutat om det i ett enskilt fall.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Ingen remissinstans invänder mot utredningens förslag.

Skälen för regeringens förslag: Enligt gällande rätt 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 (1 kap. 14 § FM-PuL och FRA-PuL). Regeringen har meddelat föreskrifter om 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 och 8 § FRA-PuF).

Sättet att hantera stora volymer information, inbegripet personuppgifter, har genomgått stora förändringar sedan tillkomsten av FM-PuL och FRA-PuL. Huvuddelen av all informationsöverföring mellan Försvarsmakten och andra myndigheter sker för närvarande elektroniskt. Regeringen föreslog i propositionen Brottsdatalag – kompletterande lagstiftning att begränsningen till enstaka personuppgifter skulle tas bort och att personuppgifter ska få lämnas ut elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt. Ett skäl till detta var att den tidigare bestämmelsen, som hade ett motsvarande innehåll som 1 kap. 14 § FM-PuL och FRA-PuL, ansågs otidsenlig och i alltför hög grad begränsade möjligheten till att utnyttja de fördelar som elektronisk kommunikation kan ge (prop. 2017/18:269 s. 134–136). Regeringen föreslog motsvarande ordning i lagstiftningsärendet avseende ny lag om Säkerhetspolisens behandling av personuppgifter (prop. 2018/19:163 s. 97–98). En sådan

bestämmelse finns nu i de särskilda personuppgiftslagarna för bl.a. Säkerhetspolisen, Kustbevakningen och Tullverket. Regeringen bedömer, i likhet med utredningen, att Försvarsmakten bör få kunna lämna ut personuppgifter elektroniskt på annat sätt än genom direktåtkomst, om det inte är olämpligt. Föreskrifter om begränsningar av denna möjlighet kan lämpligen meddelas genom förordning.

Avseende Försvarets radioanstalt föreslår utredningen att Försvarets radioanstalt bör få lämna ut personuppgifter elektroniskt på annat sätt än genom direktåtkomst, om regeringen har meddelat föreskrifter eller har beslutat om det i ett enskilt fall. Förslaget liknar därmed mer den bestämmelse som för närvarande finns i FRA-PuL. Regeringen, som noterar att ingen remissinstans har invänt mot detta, anser att utredningens förslag bör genomföras.

Enligt *Lagrådet* ger lagförslagen i denna del intryck av att personuppgifter får lämnas ut elektroniskt om det inte är olämpligt, men att det inte ställs något sådant krav på lämplighet om utlämnandet sker genom direktåtkomst. Lagrådet föreslår därför en annan språklig utformning av paragraferna i de nya lagarna och att paragraferna ska kompletteras med vissa upplysningsbestämmelser. Regeringen anser dock att utformningen enligt lagrådsremissens förslag är tillräckligt tydligt ur ett rättstillämpningsperspektiv och därför bör stå kvar.

10.3 Direktåtkomst

10.3.1 Direktåtkomst för svenska myndigheter

Regeringens förslag: Säkerhetspolisen och Försvarets radioanstalt ska få medges direktåtkomst hos Försvarsmakten till personuppgifter som utgör bearbetningsunderlag och analysresultat inom försvarsunderrättelseverksamheten och som finns i uppgiftssamlingar.

Totalförsvarets plikt- och prövningsverk ska få medges direktåtkomst hos Försvarsmakten till personuppgifter som rör totalförsvarspliktiga och Försvarsmaktens krigsorganisation och som har gjorts gemensamt tillgängliga inom Försvarsmakten.

Säkerhetspolisen och Försvarsmakten ska få medges direktåtkomst hos Försvarets radioanstalt till personuppgifter som utgör analysresultat inom försvarsunderrättelseverksamheten och som finns i uppgiftssamlingar.

Utredningens förslag överensstämmer delvis med regeringens. Enligt utredningens förslag ska Totalförsvarets rekryteringsmyndighets direktåtkomst till personuppgifter som finns hos Försvarsmakten regleras i förordning.

Remissinstanserna: *Säkerhetspolisen*, *Polismyndigheten* och *Tullverket* välkomnar utredningens förslag. *Datainspektionen* och *Justitiekanslern* efterlyser en djupare analys av utredningens förslag. *Juridiska fakultetsstyrelsen vid Lunds universitet* efterfrågar mer restriktiva regler om direktåtkomst för svenska myndigheter. *Sveriges advokatsamfund* pekar på utmaningen i att kunna kontrollera mottagande

myndigheters behandling av de personuppgifter som har gjorts tillgängliga för dem genom direktåtkomst.

Skälen för regeringens förslag

Nuvarande möjligheter till direktåtkomst hos Försvarsmakten och Försvarets radioanstalt

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 (1 kap. 15 § första stycket FM-PuL). Sådan samverkan mellan myndigheterna sker vid Nationellt centrum för terrorhotbedömning (NCT). FRA-PuL innehåller en motsvarande bestämmelse enligt vilken Försvarets radioanstalt får medge Säkerhetspolisen och Försvarsmakten direktåtkomst (1 kap. 15 §).

Tillgången till sådana uppgifter ska enligt bestämmelserna 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 bestämmelserna gäller möjligheten att meddela föreskrifter även föreskrifter om behörighet och säkerhet vid sådan åtkomst.

Bestämmelser om direktåtkomst finns även i FM-PuF och FRA-PuF. Försvarsmakten får medge Försvarets radioanstalt direktåtkomst till uppgifter i en uppgiftssamling för försvarsunderrättelseverksamhet (8 § FM-PuF). Vidare får Försvarsmakten medge Säkerhetspolisen direktåtkomst till uppgifter i en uppgiftssamling för säkerhetsskyddstjänst. Tillgången till sådana personuppgifter ska vara förbehållen de personer inom Försvarets radioanstalt och Säkerhetspolisen som på grund av sina arbetsuppgifter behöver ha tillgång till uppgifterna (9 § FM-PuF).

Försvarets radioanstalt får med stöd av FRA-PuF medge Regeringskansliet, Säkerhetspolisen, Nationella operativa avdelningen i Polismyndigheten, Inspektionen för strategiska produkter, Försvarsmakten, Försvarets materielverk, Totalförsvarets forskningsinstitut, Myndigheten för samhällsskydd och beredskap och Tullverket direktåtkomst till uppgifter i en uppgiftsamling för underrättelser. Tillgången till uppgifterna ska vara förbehållen de personer inom myndigheterna som på grund av sina arbetsuppgifter behöver ha tillgång till uppgifterna (9 §).

Behov av att utbyta information med andra myndigheter

Försvarsmakten och Försvarets radioanstalt har behov av att utbyta information med andra myndigheter. Det kan exempelvis röra kartläggning av terrorhot och Försvarsmaktens personalförsörjning inom totalförsvaret.

Både i Sverige och inom EU uppmuntras myndigheter att i så stor utsträckning som möjligt dra nytta av de effektivitetsvinster som modern teknik kan ge. Regeringen vill i sammanhanget understryka att det endast är fråga om att ge myndigheterna ett författningsstöd för att kunna medge direktåtkomst för vissa syften. Det är Försvarsmakten och Försvarets radioanstalt som i det enskilda fallet avgör om sådan åtkomst ska medges. Det är också myndigheterna som avgör vilka uppgifter som kommer att vara tillgängliga för direktåtkomst. Vid direktåtkomst ska bestämmelser om sekretess, säkerhetsskydd och dataskydd beaktas hos Försvarsmakten och Försvarets radioanstalt, men också hos den mottagande myndigheten. Detta gäller oavsett om stödet för direktåtkomst ges i lag eller förordning.

Eftersom det nu är fråga om att i författning ge viss ökad möjlighet för direktåtkomst för vissa svenska myndigheter kan det, som *Juridiska fakultetsstyrelsen vid Lunds universitet* efterfrågar, övervägas om regleringen, med avsteg från utredningens förslag, bör utformas mer restriktivt avseende möjligheten att medge andra svenska myndigheter direktåtkomst till vissa personuppgifter vid Försvarsmakten och Försvarets radioanstalt. Det är viktigt att myndigheterna ges möjlighet att utföra sina uppgifter effektivt, med beaktande av den enskildes integritet och gällande säkerhetsskyddskrav. Regeringen anser att utredningens förslag säkerställer en sådan balans och ser inte behov av att, utöver vad som anförs ovan, införa ytterligare begränsningar av det slag som Juridiska fakultetsstyrelsen vid Lunds universitet efterfrågar.

Sveriges advokatsamfund pekar på utmaningen i att kunna kontrollera mottagande myndigheters behandling av de personuppgifter som har gjorts tillgängliga för dem genom direktåtkomst. Regeringen vill med anledning av detta på nytt understryka att omfattningen av direktåtkomst bestäms av Försvarsmakten respektive Försvarets radioanstalt, med beaktande av tillämpliga bestämmelser om sekretess, säkerhetsskydd och dataskydd. Mottagande myndigheter ska behandla de mottagna personuppgifterna i enlighet med för dem gällande dataskyddsregelverk. Skulle det visa sig att en mottagande myndighet inte behandlar personuppgifter i enlighet med gällande rätt kan ansvarig tillsynsmyndighet ingripa med bl.a. sanktioner. I en sådan eventuell situation skulle dessutom möjligheten till direktåtkomst avbrytas av Försvarsmakten respektive Försvarets radioanstalt till dess att den mottagande myndigheten har vidtagit lämpliga åtgärder för att kunna uppfylla de krav som gäller.

Regeringen gör sammantaget bedömningen att det bör vara möjligt för Försvarsmakten och Försvarets radioanstalt att i den utsträckning som följer av lag och förordning medge direktåtkomst till svenska myndigheter.

Val av regleringsform

Direktåtkomst till uppgifter hos Försvarsmakten och Försvarets radioanstalt regleras för närvarande i förordning, med undantag för direktåtkomst inom samarbetet NCT som regleras i lag. I propositionen Ett mer effektivt informationsutbyte vid Nationellt centrum för terrorhotbedömning bedömde regeringen att ett möjliggörande av direktåtkomst som form för utlämnande av uppgifter mellan myndigheterna 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 RF. Regeringen ansåg emellertid ändå att det framstod som mest ändamålsenligt att i det aktuella fallet 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 faktiskt införs. Vid valet av regleringsform för Försvarsmaktens och Försvarets radioanstalts vidkommande beaktades också att Säkerhetspolisens utlämnande av uppgifter genom direktåtkomst skulle regleras i lag (prop. 2017/18:36 s. 26–28).

På samma sätt som vid införandet av FM-PuL och FRA-PuL bedömer regeringen att det inte är lämpligt att detaljreglera Försvarsmaktens och Försvarets radioanstalts verksamheter i lag. Om lagreglering inte krävs och det inte heller finns andra omständigheter som talar för en reglering i lag kan direktåtkomst lämpligen regleras i förordning.

Direktåtkomst för Säkerhetspolisen och Försvarets radioanstalt i Försvarsmaktens försvarsunderrättelseverksamhet

Försvarsmakten och Försvarets radioanstalt har 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.

Försvarsmakten och Försvarets radioanstalt 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 utvecklingen under de senaste åren. Samarbetet leder till att myndigheterna delger varandra underrättelser. Några hinder i form av sekretess föreligger typiskt sett 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.

Den föreslagna möjligheten till informationsutbyte mellan myndigheterna innebär att uppgifter från Försvarsmakten blir tillgängliga utanför det sammanhang där de ursprungligen behandlades. Sammanhanget skiljer sig dock inte nämnvärt när det gäller den underrättelseverksamhet som de tre myndigheterna har till uppgift att bedriva till skydd för Sveriges försvar och säkerhet. Ur ett integritetsskyddsperspektiv bör direktåtkomst dock endast kunna medges till uppgifter som är gemensamt tillgängliga i Försvarsmaktens

verksamhet. Från ett integritetsskyddsperspektiv är det vidare en fördel om det tydligt framgår av författningstexten vilka uppgifter som får lämnas ut genom direktåtkomst.

Möjlig direktåtkomst för Säkerhetspolisen och Försvarets radioanstalt till Försvarsmaktens personuppgifter bör avse personuppgifter som utgör bearbetningsunderlag och analysresultat inom försvarsunderrättelseverksamheten och som finns i uppgiftssamlingar. Den föreslagna bestämmelsen ersätter nuvarande 1 kap. 15 § FM-PuL som primärt avser samarbetet NCT. Även om direktåtkomsten inte längre knyts till NCT-samarbetet utgör det samarbetet även fortsatt ett viktigt forum där möjligheten till direktåtkomst kommer att användas. Det faktum att förslaget innebär en något vidgad möjlighet till direktåtkomst för Säkerhetspolisen och Försvarets radioanstalt medför inte att regeringen nu gör någon annan bedömning i förhållande till 2 kap. 6 § andra stycket RF än den som görs i prop. 2017/18:36. Med hänsyn till att nuvarande bestämmelse finns i lag är det dock lämpligt att även den nya bestämmelsen anges i lag. Om det finns behov av att begränsa omfattningen av direktåtkomsten ytterligare kan det göras i förordning eller i myndighetsinterna föreskrifter.

Direktåtkomst för Totalförsvarets plikt- och prövningsverk till personuppgifter hos Försvarsmakten som rör totalförsvarspliktiga

Utredningen föreslår att Totalförsvarets plikt- och prövningsverk (f.d. Totalförsvarets rekryteringsmyndighet) ska få medges direktåtkomst till vissa personuppgifter som Försvarsmakten behandlar. Det får endast vara fråga om personuppgifter som rör totalförsvarspliktiga och Försvarsmaktens krigsorganisation, och som har gjorts gemensamt tillgängliga. Regeringen anser i likhet med utredningen att det bör vara möjligt för Försvarsmakten att kunna medge direktåtkomst till Totalförsvarets plikt- och prövningsverk. Totalförsvarets plikt- och prövningsverk med sitt särskilda ansvar för totalförsvarspliktiga, har behov av att på ett enkelt och effektivt sätt ha tillgång till nu aktuella personuppgifter hos Försvarsmakten.

Enligt totalförsvarsdatalagen får Försvarsmakten medges direktåtkomst till personuppgifter hos Totalförsvarets plikt- och prövningsverk. Regeringen eller den myndighet regeringen bestämmer kan med stöd av 8 kap. 7 § RF meddela ytterligare föreskrifter om begränsningar av direktåtkomsten och föreskrifter om behörighet och säkerhet vid sådan åtkomst (12 §). I samma lag finns även en sekretessbrytande bestämmelse som anger att Försvarsmakten har rätt att vid direktåtkomsten ta del av de personuppgifter som omfattas av åtkomsten (13 §).

Mot den bakgrunden anser regeringen att Totalförsvarets plikt- och prövningsverks direktåtkomst till vissa personuppgifter hos Försvarsmakten bör regleras i lag och inte i förordning, som utredningen föreslår. Däremot kan typen av personuppgifter och frågor om behörighet och säkerhet lämpligen regleras i förordning på samma sätt som enligt totalförsvarsdatalagstiftningen. Totalförsvarets plikt- och prövningsverk bör alltså få medges direktåtkomst till personuppgifter i Försvarsmakten som rör totalförsvarspliktiga och Försvarsmaktens krigsorganisation och som har gjorts gemensamt tillgängliga inom Försvarsmakten.

För Försvarets radioanstalt finns en motsvarande reglering i 1 kap. 15 § FRA-PuL som beskrivs ovan för Försvarsmakten inom NCT-samarbetet. Regeringen anser att motsvarande skäl motiverar att Säkerhetspolisen och Försvarsmakten bör få medges direktåtkomst till personuppgifter som utgör analysresultat inom Försvarets radioanstalts försvarsunderrättelseverksamhet och som finns i uppgiftssamlingar.

Direktåtkomst för svenska myndigheter i andra situationer

Regeringen kan med stöd av 8 kap. 7 § RF meddela föreskrifter om vilka som i andra fall än de som omfattas av förslagen ovan får ha direktåtkomst till gemensamt tillgängliga uppgifter. Regeringen får enligt förslaget även besluta om detta i ett enskilt fall.

Direktåtkomst som kan komma i fråga att regleras i förordning avser sådana uppgifter och syften som inte förutsätter reglering i lag. Regeringen ser inte heller att det av andra skäl finns anledning att i de nya lagarna reglera frågan om ytterligare direktåtkomst för svenska myndigheter till personuppgifter som finns hos Försvarsmakten och Försvarets radioanstalt. Regeringen vill i sammanhanget understryka att bestämmelser om direktåtkomst alltid måste föregås av noggranna överväganden oavsett om regleringen ska tas in i lag eller förordning.

Omfattningen av direktåtkomsten

Omfattningen av den direktåtkomst som möjliggörs genom förslaget, samt dokumentations- och användarkrav hos mottagaren, kan lämpligen regleras närmare i förordning.

10.3.2 Direktåtkomst för utländska myndigheter och internationella organisationer

Regeringens förslag: Om det behövs för samarbetet mot terrorism eller vid svenskt deltagande i annat internationellt underrättelse- och säkerhetssamarbete ska en utländsk underrättelse- eller säkerhetstjänst få medges direktåtkomst hos Försvarsmakten till personuppgifter som behandlas i försvarsunderrättelseverksamheten och som finns i uppgiftssamlingar.

Om det behövs för samarbetet mot säkerhetshotande verksamhet som riktas mot Försvarsmakten och dess säkerhetsintressen ska en utländsk underrättelse- eller säkerhetstjänst få medges direktåtkomst hos Försvarsmakten till personuppgifter som behandlas i den militära säkerhetstjänsten och som finns i uppgiftssamlingar.

Om det behövs för samarbetet mot terrorism eller för annat internationellt säkerhetssamarbete ska en utländsk underrättelse- eller säkerhetstjänst få medges direktåtkomst hos Försvarets radioanstalt till personuppgifter som behandlas i försvarsunderrättelseverksamheten och som finns i uppgiftssamlingar.

Om det behövs för samarbetet mot it-relaterade hot mot samhällsviktiga system får en utländsk organisation inom informations-

säkerhetsområdet medges direktåtkomst hos Försvarets radioanstalt till personuppgifter som behandlas i informationssäkerhetsverksamheten och som finns i uppgiftssamlingar.

Direktåtkomst ska bara få medges i den utsträckning som följer av lag eller förordning eller om regeringen har beslutat om det i ett enskilt fall.

Utredningens förslag överensstämmer delvis med regeringens. Enligt utredningens förslag ska direktåtkomst i vissa fall regleras i förordning.

Remissinstanserna: *Statens inspektion för försvarsunderrättelseverksamheten* anser att utredningens förslag skapar risk för ett ökat integritetsintrång för enskilda. *Juridiska fakultetsstyrelsen vid Lunds universitet* efterfrågar mer restriktiva regler om direktåtkomst för utländska myndigheter och internationella organisationer.

Skälen för regeringens förslag

En ny möjlighet för direktåtkomst i det internationella samarbetet

I förarbetena till FM-PuL och FRA-PuL gjorde regeringen bedömningen att direktåtkomst för andra än svenska myndigheter inte kunde komma i fråga. Skälen för det ställningstagandet var den avvägning som måste göras mellan hänsynen till myndigheternas effektivitet, å ena sidan, och de registrerades integritet, å andra sidan. Vid den avvägningen måste också beaktas den sekretess och säkerhet i övrigt som gäller inom Försvarsmaktens och Försvarets radioanstalts aktuella verksamheter och att myndigheternas information inte sprids till obehöriga (prop. 2006/07:46 s. 80).

Sedan dess har det internationella samarbetet inom försvars- och säkerhetsområdet ökat. Den tekniska utvecklingen har också lett till att en nödvändig skyddsnivå för den utlämnande myndighetens system och personuppgifter, vilken tidigare har ansetts svår att uppnå, numera är möjlig att säkerställa. Som utredningen föreslår bör det därför nu införas en möjlighet för Försvarsmakten och Försvarets radioanstalt att kunna medge direktåtkomst för utländska myndigheter och internationella organisationer.

Den fortsatta tekniska utvecklingen medför att de tekniska förutsättningarna för att möjliggöra direktåtkomst ökar. Försvarsmakten och Försvarets radioanstalt måste dock alltjämt, enligt bl.a. gällande bestämmelser om sekretess, säkerhetsskydd och dataskydd, på förhand bedöma om direktåtkomst bör medges en utländsk aktör. Några mer restriktiva bestämmelser av det slag som *Juridiska fakultetsstyrelsen vid Lunds universitet* efterfrågar är enligt regeringen därför inte nödvändiga.

Försvarsmaktens och Försvarets radioanstalts internationella försvarsunderrättelsesamarbete

Utvecklingen i Sverige och i omvärlden skärper kraven på Sveriges förmåga att värna sin säkerhet. Detta gäller inte minst på området försvarsunderrättelseverksamhet, där internationell samverkan i många fall är helt nödvändig för att Försvarsmakten och Försvarets radioanstalt ska kunna lösa sina uppgifter. Direktåtkomst kommer endast i fråga mellan underrättelsefunktioner som redan är delaktiga i ett tätt och interaktivt samarbete inom ramen för de utländska förhållanden som

försvarsunderrättelseverksamheten inriktas mot. De personuppgifter som överförs och kommer att överföras genom t.ex. direktåtkomst är sådana som bedömts vara relevanta för gemensamma underrättelseområden.

Samarbete sker t.ex. genom att utbyta information vid fysiska möten eller genom elektroniskt utlämnande av meddelanden och rapporter. I de fall där samarbete i hög grad förutsätter 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. En sådan situation 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 utländsk myndighet. I sådana fall är det angeläget att kunna tillgängliggöra ett samlat kunskapsläge över tid. En möjlighet bör, som utredningen föreslår, kunna vara att Försvarsmakten och Försvarets radioanstalt medger en utländsk myndighet direktåtkomst till en uppgiftssamling som etablerats specifikt för ett sådant samarbete.

Om det behövs för samarbetet mot terrorism eller vid svenskt deltagande i annat internationellt underrättelse- och säkerhetssamarbete bör därför, i den utsträckning det följer av lag eller förordning eller om regeringen har beslutat om det i ett enskilt fall, en utländsk underrättelse- eller säkerhetstjänst få medges direktåtkomst till personuppgifter som behandlas i Försvarsmaktens respektive Försvarets radioanstalts försvarsunderrättelseverksamhet och som finns i uppgiftssamlingar.

Försvarsmaktens internationella säkerhetstjänstsamarbete

Försvarsmakten har även i sin militära säkerhetstjänst ett behov av att kunna dela med sig av information i samarbetet med underrättelse- eller säkerhetstjänster i andra länder. Enligt Försvarsmaktens bedömning kan myndigheten 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.

Som utredningen föreslår bör det införas en bestämmelse om direktåtkomst vid Försvarsmaktens internationella säkerhetstjänstsamarbete. Med hänsyn till att den möjliga direktåtkomsten rör uppgifter i Försvarsmaktens militära säkerhetstjänst inom ramen för internationellt samarbete anser regeringen att den lämpligen bör tas in i den nya lagen och inte i förordning, som utredningen föreslår.

Regeringen föreslår därför att en utländsk underrättelse- eller säkerhetstjänst bör få medges direktåtkomst till personuppgifter hos Försvarsmakten som behandlas i den militära säkerhetstjänsten och som finns i uppgiftssamlingar. Sådan direktåtkomst ska dock bara få medges i den utsträckning det följer av lag eller förordning eller om regeringen har beslutat om det i ett enskilt fall.

Försvarets radioanstalts internationella informationssäkerhetssamarbete

Utvecklingen på informationssäkerhetsområdet 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. Känne-

tecknande 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.

Informationssäkerhet syftar till att på olika sätt möjliggöra skydd för Sverige och svenska intressen och motverka hot mot svenska liv, hot mot svensk konfidentiell information och hot mot svensk kritisk infrastruktur. De personuppgifter som inhämtas inom ramen för denna verksamhet innebär inte en sådan övervakning eller kartläggning av enskilda som enligt regeringsformen ställer krav på reglering i lag. Med hänsyn till att det är fråga om att möjliggöra direktåtkomst för utländska myndigheter och internationella organisationer till vissa uppgiftssamlingar vid Försvarets radioanstalt är det emellertid lämpligt att stöd för detta ges i den nya lagen.

Mot denna bakgrund bör det, i enlighet med utredningens förslag, 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 har beslutat om det i ett enskilt fall.

Omfattningen av direktåtkomsten

Den närmare omfattningen av den direktåtkomst som möjliggörs genom förslaget, samt dokumentations- och användarkrav hos mottagaren, kan lämpligen regleras i förordning.

10.4 Sekretessbrytande bestämmelser

10.4.1 Varför behövs sekretessbrytande bestämmelser?

Sekretess hos Försvarsmakten och Försvarets radioanstalt

De personuppgifter som Försvarsmakten och Försvarets radioanstalt behandlar omfattas som regel av utrikes- eller försvarssekretess enligt 15 kap. 1 och 2 §§ offentlighets- och sekretesslagen (2009:400). Utrikessekretess och försvarssekretess avser att skydda allmänna intressen. Utrikessekretess gäller bl.a. för uppgifter som rör Sveriges förbindelser med en annan stat eller en mellanfolklig organisation. Försvarssekretess gäller för uppgifter om det militära försvaret, totalförsvaret och rikets säkerhet.

Uppgifter om enskilda i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst och Försvarets radioanstalts underrättelse- och säkerhetsverksamhet omfattas som regel av sekretess enligt 38 kap. 4 § offentlighets- och sekretesslagen. Enligt paragrafen gäller sekretess inom dessa verksamheter 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 denne lider skada eller men. Uppgifter om enskilda som förvaras hos Försvarsmakten kan även omfattas av sekretess enligt 38 kap. 1 § offentlighets- och

sekretesslagen. Enligt den bestämmelsen gäller sekretess för uppgifter som förekommer i ärende som t.ex. angår antagning till utbildning vid Försvarsmakten. Sekretessen gäller dock inte beslut i ärende.

Sekretess mellan myndigheter

Försvarsunderrättelseverksamhet bedrivs av Försvarsmakten, Försvarets radioanstalt, Försvarets materielverk och Totalförsvarets forskningsinstitut (se 2 § förordningen om försvarsunderrättelseverksamhet). Försvarsmakten och Försvarets radioanstalt samarbetar bl.a. med Säkerhetspolisen i frågor som rör Sveriges säkerhet. Sekretess gäller i större eller mindre utsträckning för åtskilliga av de personuppgifter som behandlas inom dessa verksamheter.

Enligt 8 kap. 1 § offentlighets- och sekretesslagen får uppgifter för vilka sekretess gäller inte röjas för andra myndigheter, om inte annat framgår av den lagen eller lag eller förordning till vilken lagen hänvisar. När uppgifter ska lämnas mellan myndigheter måste därför hänsyn tas till offentlighets- och sekretesslagstiftningen. Motsvarande begränsning gäller vid uppgiftslämnande mellan olika verksamhetsgrenar inom en myndighet, när dessa är att betrakta som självständiga i förhållande till varandra.

Offentlighets- och sekretesslagen innehåller bestämmelser som möjliggör utbyte av uppgifter mellan myndigheter utan hinder av sekretess. Av 10 kap. 2 § offentlighets- och sekretesslagen framgår att sekretess inte hindrar att uppgifter lämnas till en annan myndighet, om det är nödvändigt för att den utlämnande myndigheten ska kunna fullgöra sin verksamhet. Bestämmelsen, som är avsedd att tillämpas restriktivt, medger inte sekretessgenombrott på den grunden att den mottagande myndigheten behöver uppgifterna i sin verksamhet. Enligt 10 kap. 28 § första stycket offentlighets- och sekretesslagen hindrar sekretess inte att uppgifter lämnas till en annan myndighet om uppgiftsskyldighet följer av lag eller förordning. Enligt den s.k. generalklausulen i 10 kap. 27 § offentlighets- och sekretesslagen gäller som huvudregel att en uppgift får lämnas ut till en annan myndighet, om det är uppenbart att intresset av att uppgiften lämnas ut har företräde framför det intresse som sekretessen ska skydda.

Förhållandet mellan direktåtkomst och sekretess

En bestämmelse om direktåtkomst reglerar endast tillåtligheten av ett visst tillvägagångssätt för att lämna ut uppgifter. En sådan bestämmelse har alltså inte någon sekretessbrytande effekt, den innebär inte en uppgiftsskyldighet enligt 10 kap. 28 § första stycket offentlighets- och sekretesslagen. Möjligheterna för t.ex. en myndighet att vid informationsutbyte med en annan myndighet överföra uppgifter genom att medge direktåtkomst till uppgifter som behandlas automatiserat begränsas därför inte sällan av sekretess. Eftersom direktåtkomst innebär att den mottagande myndigheten fritt kan avgöra vilka uppgifter – inom ramen för den beviljade direktåtkomsten – som den vill ta del av, anses uppgifterna utlämnade i och med att direktåtkomst medges. Det saknar betydelse om den mottagande myndigheten faktiskt tar del av en viss uppgift eller inte. 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. Direktåtkomst förutsätter därför att det är fråga om offentliga uppgifter, uppgifter som omfattas av en bestämmelse om uppgiftsskyldighet eller att det finns en annan sekretessbrytande bestämmelse som ger stöd för att uppgiften kan lämnas ut.

Sekretess i förhållande till en utländsk aktör

Uppgifter som omfattas av sekretess får som huvudregel inte röjas för en utländsk myndighet eller en mellanfolklig organisation. Det finns dock vissa undantag från denna huvudregel bl.a. om utlämnandet görs i enlighet med särskild föreskrift i lag eller förordning (8 kap. 3 § 1 offentlighets- och sekretesslagen). Sådana föreskrifter finns t.ex. i 6 § FM-PuF och 7 § FRA-PuF. Enligt bestämmelserna får uppgifter lämnas ut till en utländsk myndighet eller en internationell organisation, om utlämnandet tjänar den svenska statsledningen eller det svenska totalförsvaret. De uppgifter som Försvarsmakten och Försvarets radioanstalt lämnar till andra länder eller internationella organisationer får inte vara till skada för svenska intressen.

10.4.2 Sekretessbrytande bestämmelser gentemot svenska myndigheter

Regeringens förslag: Försvarets radioanstalt, Säkerhetspolisen och Totalförsvarets plikt- och prövningsverk ska ha rätt att vid direktåtkomst hos Försvarsmakten ta del av de personuppgifter som omfattas av åtkomsten.

Försvarsmakten och Säkerhetspolisen ska ha rätt att vid direktåtkomst hos Försvarets radioanstalt ta del av de personuppgifter som omfattas av åtkomsten.

Utredningens förslag stämmer delvis överens med regeringens. Utredningen föreslår sekretessbrytande bestämmelser för Försvarsmakten respektive Försvarets radioanstalt samt Säkerhetspolisen för uppgifter som omfattas av sekretess enligt 38 kap. 4 § offentlighets- och sekretesslagen.

Remissinstanserna: *Försvarsmakten* och *Polismyndigheten* framhåller vikten av sekretessbrytande bestämmelser.

Skälen för regeringens förslag

Sekretessen behöver kunna brytas

Försvarsmakten och Försvarets radioanstalt ska enligt förslaget ges möjlighet att lämna ut personuppgifter till varandra och till Säkerhetspolisen genom direktåtkomst (avsnitt 10.3.1). Eftersom de uppgifter som Försvarsmakten och Försvarets radioanstalt behandlar i sina verksamheter som regel omfattas av sekretess behövs det bestämmelser som bryter sekretessen för att utlämnandet genom direktåtkomst ska bli effektivt. I annat fall måste det göras en sekretessprövning i varje enskilt fall innan uppgifterna görs tillgängliga för direktåtkomst. En bestämmelse om direktåtkomst reglerar endast själva formen för utlämnandet, dvs. på vilket sätt uppgifterna får lämnas ut, och är inte en sådan uppgiftsskyldighet som har sekretessbrytande verkan enligt 10 kap. 28 §

offentlighets- och sekretesslagen. Bestämmelser om direktåtkomst kompletteras därför ofta med sekretessbrytande bestämmelser som utformas som uppgiftsskyldigheter på det sätt som avses i bestämmelsen. Det bör därför finnas sådana bestämmelser för att utlämnandet genom direktåtkomst ska bli effektivt.

Det finns bestämmelser om sekretessgenombrott som kan bli tillämpliga inom ramen för Försvarsmaktens och Försvarets radioanstalts försvarsunderrättelseverksamhet. Av lagen om försvarsunderrättelseverksamhet följer att försvarsunderrättelsemyndigheterna ska rapportera underrättelser till berörda myndigheter (2 § andra meningen). Bestämmelsen har sekretessbrytande verkan, men avser endast underrättelser. Vidare innehåller FM-PuL en sekretessbrytande bestämmelse som endast är tillämplig inom samarbetet NCT i vilket Försvarsmakten, Försvarets radioanstalt och Säkerhetspolisen deltar (1 kap. 15 a §). FRA-PuL innehåller en motsvarande sekretessbrytande bestämmelse (1 kap. 15 § a). Bestämmelserna bryter den sekretess som gäller för skyddet för enskildas personliga eller ekonomiska förhållanden inom bl.a. Försvarsmaktens och Försvarets radioanstalts försvarsunderrättelseverksamhet (38 kap. 4 § offentlighets- och sekretesslagen).

När det gäller uppgifter om totalförsvarspliktiga finns det en sekretessbrytande bestämmelse avseende journalhandlingar som upprättats under viss grundutbildning för värnplikt eller civilplikt och som senast efter avslutad utbildning ska lämnas till Totalförsvarets plikt- och prövningsverk (3 kap. 15 § förordningen [1995:238] om totalförsvarsplikt).

Vilken slags sekretess kan behöva brytas?

Frågan är vilken slags sekretess som behöver brytas för att Försvarsmakten och Försvarets radioanstalt ska kunna lämna ut uppgifter genom direktåtkomst. Nedan beskrivs sekretessbestämmelser som kan komma i fråga.

Utrikessekretess gäller för uppgift som rör Sveriges förbindelser med en annan stat eller i övrigt rör bl.a. annan stat eller mellanfolklig organisation om det kan antas att det stör Sveriges mellanfolkliga förbindelser eller på annat sätt skadar landet om uppgiften röjs (15 kap. 1 § offentlighets- och sekretesslagen). Försvarssekretess gäller för uppgift som rör verksamhet för att försvara landet eller planläggning eller annan förberedelse av sådan verksamhet eller i övrigt rör totalförsvaret, om det kan antas att det skadar landets försvar eller på annat sätt vållar fara för rikets säkerhet om uppgiften röjs (15 kap. 2 § offentlighets- och sekretesslagen).

Med hänsyn till de skyddssyften som utrikes- och försvarssekretessen har och Försvarsmaktens, Försvarets radioanstalts och Säkerhetspolisens uppgifter i fråga om Sveriges säkerhet bör det enligt regeringens mening i många fall inte medföra någon fara för rikets säkerhet eller innebära någon skada för verksamhet, eller annan skada enligt sekretessbestämmelserna, att sådana uppgifter som Försvarsmakten anser bör göras tillgängliga för Försvarets radioanstalt och Säkerhetspolisen lämnas ut till dessa myndigheter. Motsvarande bedömning gäller för när det är Försvarets radioanstalt som ansvarar för att medge direktåtkomst. Skaderekvisitet är då inte uppfyllt och något generellt behov av att bryta sekretessen enligt

dessa bestämmelser kan inte anses föreligga. I de fall utlämnandet av en uppgift till någon av de aktuella myndigheterna skulle innebära att Försvarsmaktens eller Försvarets radioanstalts egen verksamhet riskerar att skadas, bör direktåtkomst givetvis inte komma i fråga.

Uppgifter om enskildas personliga och ekonomiska förhållanden som förekommer i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst eller i Försvarets radioanstalts underrättelse- och säkerhetsverksamhet omfattas som regel av sekretess enligt 38 kap. 4 § offentlighets- och sekretesslagen. Utlämnande av sådana uppgifter kan i de flesta fall typiskt sett anses vara till skada eller men för den enskilde. Om sådana uppgifter ska lämnas ut måste dessutom en sekretessprövning göras i varje enskilt fall. Det är inte möjligt att på förhand göra en generell intresseavvägning i fråga om sådana uppgifter. För att Försvarsmakten och Försvarets radioanstalt ska kunna utbyta den typen av uppgifter med varandra genom direktåtkomst, krävs det därför att sekretessen bryts. Detta krav gäller även vid Säkerhetspolisens direktåtkomst till uppgifter som finns hos Försvarsmakten eller Försvarets radioanstalt.

Försvarsmaktens uppgiftsskyldighet gentemot Totalförsvarets plikt- och prövningsverk rör personalförsörjningen av totalförsvaret. De sekretessbestämmelser som kan aktualiseras är främst försvarssekretess enligt 15 kap. 2 §, och när det gäller skyddet av totalförsvarspliktigas personliga förhållanden, inskrivning och krigsplacering, personalvård och utbildning för totalförsvarsändamål, 38 kap. 1–3 §§ offentlighets- och sekretesslagen. Bestämmelserna tillämpas av båda myndigheterna.

Bestämmelser om uppgiftsskyldighet bör införas

Sekretessbrytande bestämmelser i form av uppgiftsskyldighet utformas inte sällan som en rätt för mottagaren att ta del av vissa uppgifter, se t.ex. 13 § totalförsvarsdatalagen. Regeringen anser, till skillnad från utredningen, att de sekretessbrytande bestämmelserna i de nya lagarna bör utformas på motsvarande sätt. Uppgiftsskyldigheten bör omfatta sådana uppgifter som de mottagande myndigheterna får ta del av genom direktåtkomst (avsnitt 10.3.1).

Regeringens förslag innebär att sekretessgenombrott ska tillåtas i vissa fall. Bestämmelsen om utlämnande måste emellertid ses tillsammans med hur regelsystemet i övrigt har utformats. För det första bör utlämnandet bara få avse uppgifter som har gjorts gemensamt tillgängliga. Detta innebär i sig en begränsning, eftersom många av de uppgifter som Försvarsmakten och Försvarets radioanstalt behandlar aldrig kommer att göras gemensamt tillgängliga. För behandlingen av gemensamt tillgängliga uppgifter ska, som framgår av avsnitt 9, gälla särskilda begränsningar, vilket bl.a. innebär att enligt huvudregeln bara vissa typer av uppgifter ska vara åtkomliga vid sökning. Om direktåtkomst medges, kommer dessutom tillgången till olika typer av uppgifter att begränsas genom behörighetsregler. När en uppgift blir åtkomlig för en tjänsteman vid en annan myndighet kommer den myndighetens registerförfattning att bli tillämplig, vilken i likhet med vad som gäller för Försvarsmakten och Försvarets radioanstalt innehåller bestämmelser som syftar till att minska risken för integritetsintrång. Den sekretessbrytande bestämmelsen måste också ses tillsammans med bestämmelserna om att tillgången till

personuppgifter ska begränsas till vad den enskilde tjänstemannen behöver för att fullgöra sina arbetsuppgifter. Förslaget skapar förutsättningar för bättre informationsutbyte mellan de aktuella myndigheterna, samtidigt som risken för integritetsintrång beaktas. Det bör framgå av den nya lagen att regeringen har möjlighet att meddela föreskrifter om att uppgifter får lämnas ut även i andra fall än de som redovisas ovan.

Polismyndigheten framhåller behovet av sekretessbrytande bestämmelser. Regeringen anser att, i de fall det behövs sekretessbrytande bestämmelser för svenska myndigheters direktåtkomst till personuppgifter hos Försvarsmakten och Försvarets radioanstalt i andra fall än de som nu föreslås regleras i lag, kan detta lämpligen regleras i förordning.

10.5 Överföring av personuppgifter till andra länder och internationella organisationer

Regeringens förslag: Försvarsmakten får föra över personuppgifter till ett annat land eller en internationell organisation 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 om att överföring får ske även i andra fall om det är nödvändigt för verksamheten vid Försvarsmakten.

Regeringen får också besluta om sådan överföring i ett enskilt fall.

Försvarets radioanstalt får föra över personuppgifter till ett annat land eller en internationell organisation endast om det är nödvändigt för att Försvarets radioanstalt ska kunna fullgöra sina uppgifter inom ramen för det internationella försvarsunderrättelse- och säkerhetssamarbetet och

1. överföringen riktas till en utländsk underrättelse- eller säkerhetstjänst, eller ett underrättelse- eller säkerhetsorgan i en internationell organisation,
2. sekretess inte hindrar en överföring, och
3. mottagaren garanterar tillräckligt skydd för personuppgifterna.

Regeringen kan meddela föreskrifter om att överföring får ske även i andra fall än när överföringen riktas till en utländsk underrättelse- eller säkerhetstjänst, eller ett underrättelse- eller säkerhetsorgan i en internationell organisation.

Regeringen får också besluta om sådan överföring i ett enskilt fall.

Utredningen om behandlingen av personuppgifter vid Försvarsmakten och Försvarets radioanstalts förslag överensstämmer med regeringens såvitt avser Försvarsmakten.

Remissinstanserna: *Sveriges advokatsamfund* pekar på den svårighet som finns att kontrollera hur en mottagande utländsk aktör kommer att behandla personuppgifter som den har mottagit. *TCO* efterfrågar regler om hur personuppgifterna får lagras, hanteras och bearbetas av utländska underrättelse- och säkerhetstjänster.

Utredningen om Försvarets radioanstalts internationella samarbetes förslag, som endast avser Försvarets radioanstalt, överensstämmer med regeringens.

Remissinstanserna: Majoriteten av remissinstanserna, däribland *Försvarets radioanstalt*, *Försvarsmakten*, *Säkerhetspolisen*, *Polismyndigheten*, *Justitiekanslern* och *Förvaltningsrätten i Stockholm*, tillstyrker eller har inga synpunkter på utredningens förslag. *Integritetsskyddsmyndigheten* anser att utredningens förslag stärker skyddet för enskildas personliga integritet. *Statens inspektion för försvarsunderrättelseverksamheten* lyfter frågan om inte rätten att behandla personuppgifter enligt utredningens förslag bör begränsas till att endast avse inhämtning och överföring av personuppgifter inom det internationella samarbetet. *Centrum för rättvisa* efterfrågar en ökad precisering av vad en tillräcklig skyddsnivå hos mottagaren innebär. *Sveriges advokatsamfund* pekar på utmaningen i att kunna kontrollera mottagarens behandling av de personuppgifter som har tillgängliggjorts den genom direktåtkomst.

Skälen för regeringens förslag

Nuvarande ordning

Personuppgifter som behandlas med stöd av FM-PuL och FRA-PuL får enligt nuvarande ordning under vissa förutsättningar föras över till andra länder eller mellanfolkliga organisationer. En grundläggande förutsättning är att en överföring är nödvändig för att Försvarsmakten och Försvarets radioanstalt ska kunna fullgöra sina uppgifter inom ramen för det internationella försvarsunderrättelse- och säkerhetssamarbetet. Det får inte heller föreligga sekretess som hindrar en överföring. Regeringen kan meddela föreskrifter eller i ett enskilt fall besluta om att överföring får ske i andra fall om det är nödvändigt för verksamheten hos Försvarsmakten och Försvarets radioanstalt (1 kap. 17 § FM-PuL och FRA-PuL). Enligt förordningen om försvarsunderrättelseverksamhet 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 (3 §). Utöver statens intresse har detta i rättstillämpningen även ansetts inbegripa intressen hos svenska företag och enskilda.

En motsvarande reglering finns för Försvarets radioanstalts internationella samarbete i utvecklingsverksamheten (9 § andra stycket lagen om signalspaning i försvarsunderrättelseverksamhet och 6 § förordningen om signalspaning i försvarsunderrättelseverksamhet).

I FM-PuF och FRA-PuF finns bestämmelser som ger Försvarsmakten respektive Försvarets radioanstalt möjlighet att lämna ut uppgifter till en utländsk myndighet eller en internationell organisation om utlämnandet tjänar den svenska statsledningen eller det svenska totalförsvaret. En ytterligare förutsättning enligt bestämmelsen är att uppgifter som Försvarets radioanstalt lämnar till andra länder och internationella organisationer inte får vara till skada för svenska intressen (6 § FM-PuF och 7 § FRA-PuF). Bestämmelserna har sekretessbrytande karaktär.

Möjligheten att kunna överföra information till utländska myndigheter och internationella organisationer är av avgörande betydelse för Försvarsmaktens och Försvarets radioanstalts verksamheter. Informationen innehåller inte sällan personuppgifter.

Försvarsmakten

Som Utredningen om behandlingen av personuppgifter vid Försvarsmakten och Försvarets radioanstalt föreslår bör en bestämmelse som motsvarar nuvarande reglering föras in i den nya lagen för Försvarsmakten.

För att bättre ge uttryck för den nya lagens breda tillämpningsområde anser regeringen, i likhet med utredningen, att ordet försvarsunderrättelsesamarbete inte längre bör användas utan ersättas med försvarssamarbete. Försvarsmaktens försvarsunderrättelsesamarbete är ett exempel på internationellt samarbete som faller inom ramen för myndighetens försvarssamarbete. Andra exempel är Försvarsmaktens deltagande i bilaterala och multilaterala samarbeten med andra länder inom försvarsområdet.

På motsvarande sätt som gäller enligt nuvarande reglering kan regeringen i förordning meddela föreskrifter eller i ett enskilt fall besluta om att överföring får ske i andra fall om det är nödvändigt för verksamheten hos Försvarsmakten. Ett behov av överföring av personuppgifter kan t.ex. uppkomma i myndighetens administrativa verksamhet.

Försvarets radioanstalt

I syfte att skapa ytterligare förutsebarhet för Försvarets radioanstalt i det internationella samarbetet och ett ökat skydd för den enskildes integritet, föreslår regeringen, i enlighet med Utredningen om Försvarets radioanstalts internationella samarbetes förslag, en något mer preciserad bestämmelse för Försvarets radioanstalt. Förslaget innebär att det i bestämmelsen anges särskilda villkor som ska vara uppfyllda för att en överföring av personuppgifter ska vara tillåten.

I bestämmelsen ska anges att personuppgifter endast får överföras till en utländsk underrättelse- eller säkerhetstjänst, eller ett underrättelse- eller säkerhetsorgan i en internationell organisation. EU, FN och Nato är exempel på internationella organisationer som har denna typ av organ.

På motsvarande sätt som enligt gällande rätt bör det finnas en möjlighet för regeringen att genom föreskrifter eller beslut i enskilda fall möjliggöra att överföring av personuppgifter även kan få ske i förhållande till andra internationella aktörer än dem som anges i den nya lagen. Ett sådant behov kan t.ex. uppkomma inom ramen för en internationell insats där mottagaren av Försvarets radioanstalts underrättelser är ett organ i en annan stats väpnade styrkor som inte kan sägas vara ett underrättelse- eller säkerhetsorgan (prop. 2006/07:46, s. 125 och 133).

Den nuvarande begränsningen, att en överföring av personuppgifter endast får ske om sekretess inte hindrar det, är ett villkor av grundläggande betydelse och bör även fortsatt ingå som ett villkor i bestämmelsen. De personuppgifter som Försvarets radioanstalt behandlar inom ramen för myndighetens försvarsunderrättelse- och utvecklingsverksamhet omfattas som regel av sekretess enligt 15 kap. 1 och 2 §§ offentlighets- och

sekretesslagen. Uppgifter om enskilda i sådan verksamhet omfattas också typiskt sett av sekretess enligt 38 kap. 4 § offentlighets- och sekretesslagen.

Slutligen bör krävas att en viss skyddsnivå ska vara säkerställd hos mottagaren. Det bör därför i den nya lagen införas bestämmelser som innebär ett krav på Försvarets radioanstalt att analysera och bedöma om den mottagande utländska underrättelse- eller säkerhetstjänsten eller det mottagande underrättelse- eller säkerhetsorganet i en internationell organisation erbjuder en tillräcklig skyddsnivå för de mottagna personuppgifterna.

Centrum för rättvisa efterfrågar en ökad precisering av vad en tillräcklig skyddsnivå hos mottagaren innebär. Regeringen vill med anledning av detta framhålla att det blir en fråga för Försvarets radioanstalt att göra en sammanvägd bedömning. Personuppgifter bör få överföras om Försvarets radioanstalt har tagit hänsyn till alla omständigheter kring överföringen och dragit slutsatsen att tillräckliga skyddsåtgärder för personuppgifterna föreligger. Det faktum att en mottagande stat är ansluten till dataskyddskonventionen eller en annan internationell överenskommelse som innehåller bestämmelser om dataskydd och registrerades rättigheter innebär som utgångspunkt att lämpliga skyddsåtgärder bör anses föreligga. Försvarets radioanstalt bör vidare t.ex. kunna beakta att den som ska behandla personuppgifterna i det andra landet eller i den internationella organisationen kommer att ha tystnadsplikt som omfattar de överförda uppgifterna eller att det garanteras att personuppgifterna inte kommer att behandlas för något annat ändamål än det för vilket de överförs. Även åtaganden från mottagarens sida om att inte föra personuppgifterna vidare eller att inte använda personuppgifterna efter en viss tidpunkt är omständigheter som Försvarets radioanstalt bör kunna beakta vid sin bedömning.

Ömsesidighet är av grundläggande betydelse vid internationellt samarbete. Med anledning av *Sveriges advokatsamfunds* synpunkter angående förstöringsskyldighet konstaterar regeringen att det bör ingå i den samlade bedömning som Försvarets radioanstalt ska göra inför en överföring.

I likhet med *Integritetsskyddsmyndigheten* bedömer regeringen att förslaget bidrar till att stärka integritetsskyddet för enskilda. Med hänvisning till Utredningen om Försvarets radioanstalts internationella samarbetes förslag om en ny ändamålsbestämmelse i lagen om signalspaning i försvarsunderrättelseverksamhet (se avsnitt 15.1) lyfter *Statens inspektion för försvarsunderrättelseverksamheten* frågan om inte rätten att behandla de personuppgifter som Försvarets radioanstalt har inhämtat med stöd av nämnda bestämmelse bör begränsas till vad som krävs för att inhämta och överföra personuppgifterna inom det internationella samarbetet.

Regeringen konstaterar att Försvarets radioanstalts internationella samarbete sker inom ramen för myndighetens försvarsunderrättelse- och utvecklingsverksamhet och att det, med hänsyn till de ändamål som föreslås i den nya lagen om behandling av personuppgifter vid Försvarets radioanstalt, inte finns skäl att införa ett ytterligare särskilt uttryckt ändamål för Försvarets radioanstalts behandling av personuppgifter vid internationellt samarbete. En sådan lösning skulle, som Statens inspektion

för försvarsunderrättelseverksamheten framhåller, kunna bidra till att begränsa behandlingen av aktuella personuppgifter och därmed vara integritetsskyddsstärkande. En sådan ordning riskerar dock samtidigt att påtagligt hämma Försvarets radioanstalts möjlighet att, inom ramen för det internationella samarbetet, effektivt kunna utföra försvarsunderrättelse- och utvecklingsverksamheten till nytta för Sveriges säkerhet.

Regeringen bedömer att skyddet för den enskildes integritet upprätthålls på ett fullgott sätt, dels genom den nu föreslagna lagstiftningen, dels genom regleringen i lagen om signalspaning i försvarsunderrättelseverksamhet, med krav på inriktning samt tillstånd från Försvarsunderrättelsedomstolen för Försvarets radioanstalts signalspaning, liksom Statens inspektion för försvarsunderrättelseverksamhetens kontrollverksamhet. Något behov av att införa en särskild ändamålsbestämmelse för Försvarets radioanstalts behandling av personuppgifter vid internationellt samarbete finns därför inte.

Förslaget uppfyller Europadomstolens krav enligt praxis i fråga om skydd av personuppgifter vid överföring utomlands

Europadomstolen har den 25 maj 2021 i stor sammansättning (Grand Chamber) i sitt avgörande i målet Centrum för rättvisa mot Sverige (35252/08) funnit att den svenska lagstiftningen om signalspaning i försvarsunderrättelseverksamhet i huvudsak är förenlig med Europakonventionen, men att det i några avseenden finns brister. Europadomstolen anser bl.a. att det saknas tydliga bestämmelser om att den personliga integriteten ska beaktas när Försvarets radioanstalt avser att överföra uppgifter till ett annat land. Domstolen anser vidare att det saknas ett rättsligt bindande krav för Försvarets radioanstalt att analysera och bedöma huruvida mottagaren av uppgifterna erbjuder ett tillräckligt skydd för uppgifterna (se särskilt p. 326–330 i domen).

Regeringens förslag innebär att det i den nya lagen införs bestämmelser som innebär ett krav på Försvarets radioanstalt att analysera och bedöma huruvida en utländsk mottagare av uppgifterna erbjuder ett tillräckligt skydd för dem. Regeringen anser att den brist som Europadomstolen har pekat på i detta avseende kommer att åtgärdas genom den föreslagna bestämmelsen.

Europadomstolens dom behandlas även i avsnitt 15.1.

Underrättelsesamarbete bygger på ett ömsesidigt förtroende

Sveriges advokatsamfund, *TCO* och *Centrum för rättvisa* uppmärksammar den utmaning som finns när det gäller att kontrollera hur en mottagande utländsk aktör kommer att behandla personuppgifter som den har mottagit vid ett informationsutbyte. Det kan finnas en viss grad av osäkerhet när det gäller att överföra personuppgifter till ett annat land eller en internationell organisation. Det kommer därför att även fortsatt medföra ett stort ansvar för Försvarsmakten och Försvarets radioanstalt när det gäller att bedöma i vilka fall personuppgifter kan överföras. Regeringen konstaterar att båda myndigheterna har erfarenhet av att göra denna typ av bedömningar. Den föreslagna regleringen för Försvarets radioanstalt och vad anförs ovan bidrar ytterligare till att tydliggöra vad en tillräcklig skyddsnivå hos mottagaren innebär. Regeringen vill även framhålla att

underrättelsesamarbete bygger på ett ömsesidigt förtroende. En motpart som missbrukar förtroendet kommer inte längre att få ta del av information. Det bör understrykas att Försvarsmakten och Försvarets radioanstalt inte i något fall är skyldiga att överföra personuppgifter till ett annat land eller en internationell organisation.

Närmare villkor för i vilka fall överföring av personuppgifter till utlandet ska få ske, kan på motsvarande sätt som enligt gällande rätt lämpligen regleras i förordning.

11 Personuppgiftsansvar

11.1 Vem är personuppgiftsansvarig?

Regeringens förslag: Personuppgiftsansvarig ska vara den som ensam eller tillsammans med andra bestämmer ändamålen med eller medlen för behandlingen av personuppgifter.

Försvarsmakten respektive Försvarets radioanstalt ska vara personuppgiftsansvarig för all behandling av personuppgifter som myndigheten utför, som utförs under myndighetens ledning eller på dess vägnar.

Utredningens förslag överensstämmer i sak med regeringens.

Remissinstanserna: *Datainspektionen* och *Försvarsmakten* anser att den andra meningen i utredningens lagtextförslag bör utgå då definitionen av personuppgiftsansvarig anges i de nya lagarna.

Skälen för regeringens förslag: Vad som avses med personuppgiftsansvarig definieras inte i FM-PuL och FRA-PuL. Liksom utredningen ser regeringen ett värde i att i de nya lagarna införa en sådan definition. Med personuppgiftsansvarig bör avses den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter.

I de nya lagarna bör vidare anges att Försvarsmakten respektive Försvarets radioanstalt är personuppgiftsansvarig för all behandling av personuppgifter som myndigheten utför.

Som *Lagrådet* föreslår bör det av bestämmelserna också uttryckligen framgå att personuppgiftsansvaret även inbegriper behandling av personuppgifter som utförs under myndighetens ledning eller på dess vägnar.

11.2 Ingen reglering av gemensamt personuppgiftsansvar

Regeringens bedömning: De nya lagarna bör inte innehålla någon särskild bestämmelse om gemensamt personuppgiftsansvar.

Utredningens förslag överensstämmer inte med regeringens bedömning. Utredningen föreslår att Försvarsmakten och Försvarets radioanstalt ska få vara gemensamt personuppgiftsansvariga med annan

endast i den utsträckning det följer av lag eller förordning eller om regeringen i ett enskilt fall beslutar om det.

Remissinstanserna: *Försvarets radioanstalt* välkomnar möjligheten till gemensamt personuppgiftsansvar på det sätt som utredningen föreslår. *Datainspektionen* konstaterar att utredningens förslag är en nyhet jämfört med befintliga bestämmelser. *Sveriges advokatsamfund* hänvisar till EU:s dataskyddsförordning där gemensamt personuppgiftsansvar bedöms utifrån de materiella förutsättningarna i sak.

Skälen för regeringens bedömning: Enligt förslaget ska med personuppgiftsansvarig avses den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen. Två eller flera personuppgiftsansvariga kan alltså vara gemensamt personuppgiftsansvariga för viss behandling. Ett samarbete mellan två eller flera myndigheter medför inte automatiskt ett gemensamt ansvar för behandlingen av personuppgifter. Det avgörande är i stället om de deltagande myndigheterna i någon mån tillsammans bestämmer ändamålen med och medlen för behandlingen. I många fall då myndigheter samarbetar framgår det av de faktiska omständigheterna vem som är ansvarig för vilken personuppgiftsbehandling, t.ex. genom att det endast är en myndighet som har tillgång till personuppgifterna eller it-systemet, eller om myndigheterna agerar i olika skeden av en process. Det förhållandet att två myndigheter använder samma datasystem eller att en myndighet ger en annan myndighet direktåtkomst till ett visst datasystem innebär inte heller per automatik att det uppstår ett gemensamt personuppgiftsansvar.

Utredningen föreslår att det i de nya lagarna ska tas in bestämmelser om att Försvarsmakten och Försvarets radioanstalt ska kunna vara gemensamt personuppgiftsansvariga med annan endast i den utsträckning det följer av lag eller förordning eller om regeringen i ett enskilt fall beslutar om det. Ett gemensamt personuppgiftsansvar kan då inte uppstå rent faktiskt i en viss situation, utan endast i den utsträckning som riksdagen eller regeringen har beslutat om det. Ordningen för när gemensamt personuppgiftsansvar uppkommer skulle enligt utredningen därmed bli tydligare. Vidare följer av utredningens förslag att de förpliktelser var och en av myndigheterna kommer att ha i egenskap av personuppgiftsansvarig ska regleras i en skriftlig överenskommelse och kunna följas upp av tillsyns- och kontrollmyndigheter.

Försvarets radioanstalt välkomnar utredningens förslag medan *Datainspektionen* konstaterar att förslaget är en nyhet jämfört med befintliga bestämmelser. *Sveriges advokatsamfund* pekar på att gemensamt personuppgiftsansvar enligt EU:s dataskyddsförordning bedöms utifrån de materiella förutsättningarna i sak.

Regeringen noterar att Utredningen om 2016 års dataskyddsdirektiv lämnade ett motsvarande författningsförslag i förslagen till brottsdatalag (Brottsdatalag, SOU 2017:29) och Säkerhetspolisens datalag (Brottsdatalag – kompletterande lagstiftning, SOU 2017:74). I fråga om brottsdatalagen bedömde regeringen att skillnaden mellan lydelsen i dataskyddsdirektivet och lydelsen enligt utredningens förslag skulle kunna medföra att ett gemensamt personuppgiftsansvar i vissa fall föreligger enligt direktivet men inte enligt den föreslagna lagen. Enligt regeringen kunde detta leda till oklarheter vid rättstillämpningen, särskilt med hänsyn

till att det är osäkert hur den EU-rättsliga tolkningen av begreppet gemensamt personuppgiftsansvar kan komma att utvecklas i framtiden. Regeringen bedömde därför att bestämmelsens utformning borde följa formuleringen i dataskyddsdirektivet (prop. 2017/18:232 s. 214–216). Riksdagen beslutade att anta regeringens förslag (bet. 2017/18:JuU37, rskr. 2017/18:392).

Regeringen noterar vidare att lagen (2019:1182) om Säkerhetspolisens behandling av personuppgifter inte innehåller någon bestämmelse om gemensamt personuppgiftsansvar. Med hänvisning till att det redan av definitionen av personuppgiftsansvarig följer att två eller flera kan vara gemensamt personuppgiftsansvariga, bedömde regeringen i det lagstiftningsarbetet att varken dataskyddsförordningen eller brottsdatalagen kan sägas innehålla något direkt förtydligande i denna del. Mot den bakgrunden fann regeringen inte skäl att i den nya lagen göra ett förtydligande om gemensamt personuppgiftsansvar. Regeringen konstaterade vidare att gemensamt personuppgiftsansvar kan uppkomma utan en särskild bestämmelse och att gemensamt personuppgiftsansvar torde förekomma väldigt sällan i Säkerhetspolisens verksamhet. Regeringen fann därför att det inte fanns behov av att i den nya lagen införa någon bestämmelse om gemensamt personuppgiftsansvar (prop. 2018/19:163 s. 130–132). Riksdagen beslutade att anta regeringens förslag (bet. 2019/20:JuU9, rskr. 2019/20:44).

Sammantaget anser regeringen att det är tydligt att gemensamt personuppgiftsansvar kan uppkomma om Försvarsmakten eller Försvarets radioanstalt tillsammans med någon annan aktör i Sverige eller utomlands har bestämt ändamålen med och medlen för behandlingen av personuppgifter. Detta följer redan av den föreslagna definitionen av personuppgiftsansvarig. En ordning som förutsätter ett särskilt medgivande i författning eller förvaltningsbeslut för att ett gemensamt personuppgiftsansvar ska få förekomma är således inte nödvändig för att ett sådant ansvar ska uppkomma. Utredningens förslag bör därför inte genomföras. Det bör lämpligen överlämnas till rättstillämpningen att utveckla närmare praxis kring frågan om personuppgiftsansvarets fördelning.

11.3 Skyldigheter som personuppgiftsansvarig

11.3.1 Författningsenlig behandling genom lämpliga tekniska och organisatoriska åtgärder

Regeringens förslag: Försvarsmakten och Försvarets radioanstalt ska genom lämpliga tekniska och organisatoriska åtgärder säkerställa att behandlingen av personuppgifter är författningsenlig och att den registrerades rättigheter skyddas.

Utredningens förslag överensstämmer delvis med regeringens. Utredningen föreslår bestämmelser om loggning av viss personuppgiftsbehandling hos Försvarsmakten och Försvarets radioanstalt.

Remissinstanserna: Flertalet remissinstanser tillstyrker eller invänder inte mot utredningens förslag. *Datainspektionen* anser att skyldigheten att

föra loggar inte ska begränsas till gemensamt tillgängliga uppgifter. *Försvarsmakten* framför att loggningskravet för myndigheten endast ska avse den personuppgiftsbehandling som sker i uppgiftssamlingar inom försvarsunderrättelseverksamheten och den militära säkerhetstjänsten.

Skälen för regeringens förslag: Regeringen anser i likhet med utredningen att det i de nya lagarna bör införas bestämmelser om 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.

Utredningen föreslår att de nya lagarna ska innehålla en uttrycklig bestämmelse om loggning av viss personuppgiftsbehandling hos Försvarsmakten och Försvarets radioanstalt. En logg utgör en behandlingshistorik som sparas viss tid så att åtkomsten till personuppgifterna kan kontrolleras.

Regeringen konstaterar att ansvar för loggning och logguppföljning indirekt följer av de allmänna kraven på lämpliga tekniska och organisatoriska åtgärder. Försvarsmakten och Försvarets radioanstalt för enligt gällande ordning loggar som en del i myndigheternas informationssäkerhetsarbete. EU:s dataskyddsförordning och dataskyddslagen ställer inte krav på att loggning måste ske vid behandling av personuppgifter.

Mot denna bakgrund anser regeringen att de nya lagarna inte bör innehålla uttryckliga bestämmelser om loggning. De närmare tekniska och organisatoriska åtgärder som Försvarsmakten och Försvarets radioanstalt bör vidta beror på vilken verksamhet hos de båda myndigheterna det rör sig om. Vilka närmare åtgärder som Försvarsmakten och Försvarets radioanstalt ska vidta eller vilka omständigheter som de ska beakta vid beslut om åtgärder kan lämpligen regleras i förordning.

11.3.2 Säkerheten för personuppgifter

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

Försvarsmakten och Försvarets radioanstalt ska se till att tillgången till personuppgifter begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna yttrar sig inte över utredningens förslag.

Skälen för regeringens förslag: Försvarsmakten respektive Försvarets radioanstalt ska enligt nuvarande ordning 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 (3 kap. 2 § FM-PuL och FRA-PuL). Som utredningen föreslår bör

motsvarande bestämmelser införas i de nya lagarna. Det kan i förordning anges vilka omständigheter som Försvarsmakten och Försvarets radioanstalt ska beakta vid beslut om åtgärder. Vid den bedömningen har det betydelse bl.a. vilka personuppgifter som ska behandlas, mängden uppgifter och hur integritetskänsliga uppgifterna är.

Vidare gäller att tillgången till personuppgifter alltid ska begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter (1 kap. 16 § FM-PuL och FRA-PuL. Bestämmelsen avser såväl tillgången till uppgifterna inom de berörda myndigheterna som den tillgång som personal vid andra myndigheter ges genom direktåtkomst.

Regeringen föreslår att motsvarande ska gälla enligt de nya lagarna.

11.3.3 Inget krav på en särskild konsekvensbedömning

Regeringens bedömning: Särskilda bestämmelser om konsekvensbedömningar bör inte införas i de nya lagarna.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Flertalet remissinstanser tillstyrker eller invänder inte mot utredningens bedömning.

Skälen för regeringens bedömning: EU:s dataskyddsförordning ställer krav på konsekvensbedömningar och en skyldighet för den personuppgiftsansvarige att samråda med tillsynsmyndigheten.

Enligt kraven ska konsekvenserna för skyddet av personuppgifter bedömas om en ny typ av 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 personuppgiftsansvarig myndighet samråda med tillsynsmyndigheten i god tid innan behandlingen påbörjas eller betydande förändringar genomförs. Konsekvensbedömningarna bör omfatta relevanta system och processer, men inte enskilda fall. Det ska alltså vara fråga om en typ av behandling. En konsekvensbedömning ska dokumenteras, exempelvis i en skriftlig rapport.

Regeringen bedömer att lagförslagen innebär att den personuppgiftsansvarige kontinuerligt måste bedöma konsekvenserna för skyddet av personuppgifter. Någon särskild bestämmelse om att Försvarsmakten och Försvarets radioanstalt ska genomföra en konsekvensbedömning vid behandling av personuppgifter är därför inte är nödvändig.

11.3.4 Ingen skyldighet att anmäla personuppgiftsincidenter

Regeringens bedömning: Försvarsmakten och Försvarets radioanstalt bör inte vara skyldiga att anmäla personuppgiftsincidenter till tillsynsmyndigheten.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: *Datainspektionen* och *Försvarets radioanstalt* delar utredningens bedömning att det inte bör införas en rapporteringsskyldighet av personuppgiftsincidenter. *TCO* anser att en sådan rapporteringsskyldighet bör införas.

Skälen för regeringens bedömning: Någon reglering om personuppgiftsincidenter finns inte i FM-PuL, FRA-PuL eller personuppgiftslagen. Enligt 1 kap. 4 § dataskyddslagen undantas rapportering av dataskyddsincidenter (artiklarna 33 och 34 i dataskyddsförordningen) i fråga om personuppgiftsincidenter som rapporteras enligt säkerhetsskyddslagen eller föreskrifter som har meddelats i anslutning till den lagen. Det innebär att sådana incidenter som enligt 2 kap. 10 § första stycket 2 säkerhetsskyddsförordningen ska anmälas till Säkerhetspolisen och Försvarsmakten, inte också ska rapporteras till tillsynsmyndigheten enligt dataskyddsförordningen.

Eventuella 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. Regeringen anser att det därmed inte finns något behov av att i de nya lagarna ta in bestämmelser om rapportering av personuppgiftsincidenter till tillsynsmyndigheten.

11.4 Dataskyddsombud

Regeringens förslag: Försvarsmakten och Försvarets radioanstalt ska utse ett eller flera dataskyddsombud och anmäla till tillsynsmyndigheten när dataskyddsombud utses och entledigas.

Dataskyddsombud ska ha vissa i lagarna angivna arbetsuppgifter.

Utredningens förslag överensstämmer i huvudsak med regeringens. Enligt utredningens förslag ska dataskyddsombud vara skyldiga att anmäla till tillsynsmyndigheten om personuppgiftsansvariga bryter mot bestämmelser för behandling av personuppgifter och rättelse inte vidtas. Utredningen föreslår även att dataskyddsombud ska föra en förteckning över kategorier av behandlingar som myndigheterna ansvarar för och som är helt eller delvis automatiserade.

Remissinstanserna: *Försvarets radioanstalt* anser att utredningens förslag avseende dataskyddombud är ändamålsenligt. *Datainspektionen* anser att definitionen av dataskyddsombud även bör omfatta juridiska personer. Datainspektionen anser vidare att skyldigheten att föra en förteckning över kategorier av behandlingar inte bör ligga på dataskyddsombudet utan på den personuppgiftsansvarige. *Forum för dataskydd* och *Polismyndigheten* anser att regleringen av dataskyddsombudets arbetsuppgifter bör anpassas till vad som gäller enligt annan dataskyddsreglering.

Nuvarande ordning

Enligt nuvarande ordning ska Försvarsmakten och Försvarets radioanstalt utse ett eller flera personuppgiftsombud och anmäla dessa till tillsynsmyndigheten (1 kap. 4 § FM-PuL och FRA-PuL).

Personuppgiftsombudets uppgifter anges i 4 kap. 2–4 §§ FM-PuL och FRA-PuL. Av bestämmelserna framgår att ombudet 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. Vidare ska personuppgiftsombudet 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 och även i övrigt samråda med tillsynsmyndigheten vid tveksamhet om hur de bestämmelser som gäller för behandlingen av personuppgifter ska tillämpas. Personuppgiftsombudet ska föra en förteckning över de behandlingar som Försvarsmakten genomför inom försvarsunderrättelseverksamheten respektive den militära säkerhetstjänsten och som är helt eller delvis automatiserade.

För Försvarets radioanstalt gäller motsvarande för behandlingar som myndigheten genomför och som är helt eller delvis automatiserade. Personuppgiftsombudet ska också hjälpa registrerade att få rättelse när det finns anledning att misstänka att behandlade personuppgifter är felaktiga eller ofullständiga.

Personuppgiftsombud blir dataskyddsombud

I den lagstiftning om behandling av personuppgifter som helt eller delvis bygger på unionsrätten har benämningen personuppgiftsombud ersatts av dataskyddsombud. Unionsrätten är inte tillämplig på den behandling av personuppgifter som är aktuell i detta lagstiftningsärende. Av tydlighets- och lämplighetsskäl bör dock, som utredningen föreslår, benämningen dataskyddsombud användas i även i de föreslagna lagarna.

Dataskyddsombudets uppgifter

Enligt utredningens förslag bör dataskyddsombudet ha samma uppgifter som personuppgiftsombudet har enligt FM-PuL och FRA-PuL, med undantag för skyldigheten att hjälpa registrerade att få rättelse när det finns anledning att misstänka att behandlade personuppgifter är felaktiga eller ofullständiga. Den uppgiften bör enligt utredningen ligga på den personuppgiftsansvarige. *Datainspektionen*, *Forum för dataskydd* och *Polismyndigheten* invänder mot detta med hänvisning till annan dataskyddslagstiftning.

Bestämmelserna i FM-PuL och FRA-PuL ger samma uppgifter till personuppgiftsombudet. Som Datainspektionen, Forum för dataskydd och Polismyndigheten påpekar ligger delar av detta ansvar enligt t.ex. brottsdatalagstiftningen numera på den personuppgiftsansvarige. Regeringen bedömer att dataskyddsombudets roll vid Försvarsmakten och Försvarets radioanstalt som utgångspunkt inte bör avvika i förhållande till

annan jämförbar reglering. Dataskyddsombudet bör därför självständigt kontrollera att Försvarsmakten och Försvarets radioanstalt behandlar personuppgifter författningsenligt och på ett korrekt sätt och i övrigt fullgör sina skyldigheter. Dataskyddsombudet bör vidare självständigt informera och ge råd till Försvarsmakten respektive Försvarets radioanstalt och dem som behandlar personuppgifter under myndighetens ledning om deras skyldigheter vid behandling av personuppgifter och, vid behov, söka vägledning av tillsynsmyndigheten. En kontakt med tillsynsmyndigheten bör som utgångspunkt ske först efter det att dataskyddsombudet haft kontakt med berörd enhet vid den egna myndigheten.

När det gäller ansvaret för att föra förteckningar över kategorier av behandlingar som myndigheterna ansvarar för, och som är helt eller delvis automatiserade, finns det inte skäl att göra någon åtskillnad i förhållande till annan jämförbar lagstiftning. Regeringen anser att det ansvaret därför, till skillnad från utredningens förslag, bör ligga hos den personuppgiftsansvarige. Vilka uppgifter som ska anges i en sådan förteckning kan lämpligen regleras i förordning. En kategori av behandlingar bör inte tolkas så, att alla typer av behandlingar som förekommer ska dokumenteras. En sådan tolkning skulle leda till en alltför omfattande dokumentationsskyldighet. En kategori av behandlingar kan vara behandling av personuppgifter i en särskild uppgiftssamling eller inom ramen för ett särskilt projekt eller behandling av personuppgifter för en typ av ändamål.

De föreslagna lagarna ska endast tillämpas i verksamheten hos Försvarsmakten och Försvarets radioanstalt. Detta utgör en tydlig skillnad i förhållande till brottsdatalagen som ska tillämpas av ett antal myndigheter och vissa andra aktörer som har anförtrotts en förvaltningsuppgift. Försvarsmakten och Försvarets radioanstalt bedriver verksamhet som kännetecknas av särskild reglering och krav på hög grad av it-säkerhet. Därtill kräver myndigheternas verksamheter ett väl fungerande säkerhetsskydd och de omfattas i hög grad av sekretess. Personuppgiftsbehandlingen kräver sakkunskap om verksamheten. Sett till detta och till de egenskaper och den ställning i organisationen som ett dataskyddsombud förväntas ha, anser regeringen att det saknas anledning att definitionen av dataskyddsombud i de nya lagarna även ska omfatta en juridisk person. Regeringen vill samtidigt påminna om att kravet på självständighet innebär att dataskyddsombud ska kunna utföra sina arbetsuppgifter på ett oberoende sätt. Det hindrar inte att ett dataskyddsombud även har andra arbetsuppgifter hos den personuppgiftsansvariga myndigheten. Myndigheterna måste dock utforma sin interna organisation på ett sätt som säkerställer att dataskyddsombudet kan utföra sina arbetsuppgifter som dataskyddsombud på ett oberoende sätt. Utformningen av den interna organisationen är alltså ett ansvar för den personuppgiftsansvarige.

Med anledning av vad *Forum för dataskydd* anför om att utredningens förslag kan antas ge dataskyddsombudet en mer aktiv roll med större ansvar än vad som generellt är syftet med närliggande regleringar bör det framhållas att förslaget i sak inte går längre än vad som gäller enligt nuvarande ordning. Således bör dataskyddsombud definieras som en fysisk person som utses av den personuppgiftsansvarige för att

självständigt kontrollera att personuppgifter behandlas författningsenligt och på ett korrekt sätt enligt vad som närmare anges i lagen.

Bör dataskyddsombud även ges andra arbetsuppgifter?

Personuppgiftsombud enligt FM-PuL och FRA-PuL ska hjälpa registrerade att få rättelse när det finns anledning att misstänka att behandlade personuppgifter är felaktiga eller ofullständiga. Enligt utredningens förslag ska det ansvaret i stället ligga hos den personuppgiftsansvarige.

Ett personuppgiftsombud fungerar främst som kontaktpunkt för registrerade i frågor om rättelse och är typiskt sett inte den som i praktiken rättar personuppgifter. Personuppgiftsombud används emellertid också som kontaktpunkt för registrerade i andra frågor som rör behandling av personuppgifter, t.ex. för enskilda i frågor som rör behandling av personuppgifter. Dataskyddsombuden bör ha samma roll i förhållande till enskilda som personuppgiftsombud har enligt gällande rätt. Dataskyddsombudens uppgifter i egenskap av kontaktpunkt för enskilda bör dock enligt regeringens mening inte författningsregleras.

Enligt FM-PuL och FRA-PuL ska ett personuppgiftsombud anmäla till tillsynsmyndigheten om han eller hon misstänker att den personuppgiftsansvarige bryter mot gällande bestämmelser och inte vidtar rättelse. Personuppgiftslagen innehåller en motsvarande bestämmelse. Någon sådan skyldighet följer emellertid inte av EU:s dataskyddsförordning. Lagstiftaren har därför inte funnit det motiverat att införa bestämmelser om en sådan skyldighet i brottsdatalagen (prop. 2017/18:232 s. 210, bet. 2017/18:JuU37, rskr. 2017/18:392) eller i lagen om Säkerhetspolisens behandling av personuppgifter (prop. 2018/19:163 s. 147, bet. 2019/20:JuU9, rskr. 2019/20:44).

Utredningens förslag innehåller bestämmelser om anmälningsskyldighet som motsvarar dem som för närvarande finns i FM-PuL och FRA-PuL. En sådan ordning förekommer dock inte i någon annan dataskyddsreglering. Regeringen anser därför inte att det finns skäl att införa bestämmelser om en sådan anmälningsskyldighet i de nya lagarna för Försvarsmakten och Försvarets radioanstalt.

Dataskyddsombudets möjlighet att utföra sina uppgifter ska underlättas

För att dataskyddsombuden ska kunna utföra sina arbetsuppgifter krävs det att Försvarsmakten och Försvarets radioanstalt, i deras egenskap av personuppgiftsansvariga, gör det möjligt och tillhandahåller de resurser som ombuden behöver. Myndigheterna bör t.ex. göra ombudet delaktigt i frågor som rör skyddet av personuppgifter. Ombuden bör också få tillgång till dokumentation gällande personuppgiftsbehandlingen och, i den utsträckning det behövs, tillgång till de personuppgifter som behandlas. De särskilda behörighetskrav som gäller för all verksamhet vid Försvarsmakten och Försvarets radioanstalt, inbegripet behandlingen av personuppgifter, måste även beaktas i förhållande till dataskyddsombudet.

Försvarsmakten och Försvarets radioanstalt bör se till att ombudet ges utrymme för vidareutbildning och annan kunskapsinhämtning.

Bestämmelser om vilka åtgärder den personuppgiftsansvarige måste vidta för att dataskyddsombudet ska kunna utföra sina uppgifter kan vid behov tas in i förordning.

11.5 Personuppgiftsbiträden

11.5.1 Definition av personuppgiftsbiträde

Regeringens förslag: Personuppgiftsbiträde ska i de nya lagarna definieras som den som behandlar personuppgifter för den personuppgiftsansvariges räkning.

Utredningens förslag överensstämmer delvis med regeringens. Enligt utredningens förslag ska personuppgiftsbiträde definieras som den som, med stöd av ett skriftligt avtal eller annan skriftlig överenskommelse, behandlar personuppgifter för den personuppgiftsansvariges räkning.

Remissinstanserna: *Datainspektionen* anser att det i fråga om definitionen av personuppgiftsbiträde inte ska ställas något krav på skriftligt avtal.

Skälen för regeringens förslag: Enligt FM-PuL och FRA-PuL är personuppgiftsbiträde den som behandlar personuppgifter för den personuppgiftsansvariges räkning. Enligt utredningens förslag ska med personuppgiftsbiträde i de nya lagarna avses den som, med stöd av ett skriftligt avtal eller annan skriftlig överenskommelse, behandlar personuppgifter för den personuppgiftsansvariges räkning. Den föreslagna definitionen innehåller ett uttryckligt krav på skriftligt avtal, vilket saknas i definitionen i FM-PuL och FRA-PuL. Ett sådant krav på skriftligt avtal framgår emellertid av 3 kap. 1 § FM-PuL och FRA-PuL som rör säkerheten vid behandling av personuppgifter. Ett sådant krav föreslår utredningen också ska finnas i de nya lagarna.

Utredningens förslag avviker från definitionen av personuppgiftsbiträde i EU:s dataskyddsförordning som inte innehåller krav på skriftligt avtal och *Datainspektionen* anser att definitionen inte ska innehålla något sådant krav. Till skillnad från utredningen anser regeringen inte att det finns skäl att frångå den definition av personuppgiftsbiträde som för närvarade gäller på det aktuella området och som också finns i dataskyddsförordnigen. Med personuppgiftsbiträde enligt de nya lagarna bör således avses den som behandlar personuppgifter för den personuppgiftsansvariges räkning.

Ett personuppgiftsbiträde kan vara en fysisk eller juridisk person, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning. Personuppgiftsbiträdet måste alltid finnas utanför den personuppgiftsansvariges organisation. En anställd eller någon annan som behandlar personuppgifter under den personuppgiftsansvariges direkta ansvar kan inte vara personuppgiftsbiträde.

11.5.2 Anlitande av personuppgiftsbiträden

Regeringens förslag: Försvarsmakten och Försvarets radioanstalt ska, om det är lämpligt, få anlita personuppgiftsbiträden. Innan ett personuppgiftsbiträde anlitas, ska myndigheterna 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 registrerades rättigheter.

Det ska finnas ett skriftligt avtal eller annan skriftlig överenskommelse om personuppgiftsbiträdets behandling av personuppgifter för Försvarsmaktens och Försvarets radioanstalts räkning.

Ett personuppgiftsbiträde ska inte få anlita ett annat personuppgiftsbiträde utan skriftligt tillstånd från Försvarsmakten eller Försvarets radioanstalt.

Utredningens förslag överensstämmer i sak med regeringens.

Remissinstanserna: *Försvarsmakten* anser att EU:s dataskyddsförordning är tillämplig för personuppgiftsbiträden och att en särreglering därför inte bör införas. *Juridiska fakultetsstyrelsen vid Lunds universitet* anser att det bör framgå av regleringen hur eventuella tvister mellan den personuppgiftsansvarige och personuppgiftsbiträdet ska lösas. *Sveriges advokatsamfund* anser att kraven på innehållet i personuppgiftsbiträdesavtal ska anges i lag.

Skälen för regeringens förslag: Enligt FM-PuL och FRA-PuL ska det finnas ett skriftligt avtal om personuppgiftsbiträdets behandling av personuppgifter för myndighetens räkning. I avtalet ska särskilt anges att personuppgiftsbiträdet 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 (3 kap. 1 §). Regeringen anser i likhet med utredningen, men till skillnad från *Försvarsmakten*, att motsvarande reglering bör införas i de nya lagarna.

Vidare bör i enlighet med utredningens förslag, Försvarsmakten och Försvarets radioanstalt få anlita personuppgiftsbiträden, om det är lämpligt. Frågan om det i ett enskilt fall är lämpligt att anlita ett personuppgiftsbiträde får avgöras med hänsyn bl.a. till vilka personuppgifter som ska behandlas. Som *Sveriges advokatsamfund* uppmärksammar är det också viktigt att beakta i vilken utsträckning som det gäller sekretess för personuppgifterna i fråga.

Enligt *Juridiska fakultetsstyrelsen vid Lunds universitet* bör det framgå av den nya regleringen hur eventuella tvister mellan den personuppgiftsansvarige och personuppgiftsbiträdet ska lösas. Regeringen ser inte behov av detta utan anser att det är en fråga som lämpligen kan regleras i den överenskommelse som ska ingås vid anlitande av personuppgiftsbiträde.

Till skillnad från *Sveriges advokatsamfund* anser regeringen att det närmare innehållet i en överenskommelse om anlitande av personuppgiftsbiträde lämpligen kan regleras i förordning, på motsvarande sätt som gäller för annan särskild dataskyddsreglering.

Det är av grundläggande betydelse att den personuppgiftsansvarige känner till vilka personuppgiftsbiträden som behandlat personuppgifter för dennes räkning. Som utredningen föreslår bör ett personuppgiftsbiträde

därför inte få anlita ett annat personuppgiftsbiträde utan att den personuppgiftsansvarige har lämnat skriftligt tillstånd till det.

11.5.3 Behandling enligt den personuppgiftsansvariges instruktioner

Regeringens förslag: Ett personuppgiftsbiträde och de som arbetar under biträdets ledning ska behandla personuppgifter i enlighet med instruktioner från Försvarsmakten och Försvarets radioanstalt.

Om ett personuppgiftsbiträde bestämmer ändamålen med och medlen för behandlingen ska biträdet anses vara personuppgiftsansvarig för den behandlingen.

Utredningens förslag överensstämmer i sak med regeringens.

Remissinstanserna yttrar sig inte särskilt över utredningens förslag.

Skälen för regeringens förslag: Enligt nuvarande ordning får ett personuppgiftsbiträde och den eller de personer som arbetar under biträdets eller respektive myndighets ledning behandla personuppgifter bara i enlighet med instruktioner från myndigheten (3 kap. 1 § FM-PuL och FRA-PuL). Som utredningen föreslår bör en motsvarande bestämmelse föras in i de nya lagarna.

Instruktionerna från de personuppgiftsansvariga myndigheterna bör vara så tydliga att otillåten behandling inte utförs (jfr Integritet, Offentlighet, Informationsteknik, SOU 1997:39 s. 335). Den överenskommelse som styr personuppgiftsbiträdets uppdrag ska innehålla viss information som ger instruktioner till biträdet, bl.a. om behandlingens varaktighet, art och ändamål. Instruktionerna kan också gälla exempelvis hur tillgången till personuppgifter hos biträdet ska begränsas, om biträdet ska använda kryptering vid kommunikation och andra åtgärder som krävs för att skydda personuppgifterna. Överföring av personuppgifter till tredje part eller en internationell organisation förutsätter att biträdet har fått i uppdrag att göra det. Sådana uppdrag bör också framgå av de instruktioner som den personuppgiftsansvarige lämnar till biträdet.

Att den som bestämmer ändamålen med och medlen för behandlingen är att anse som personuppgiftsansvarig framgår av den föreslagna definitionen av personuppgiftsansvarig. Regeringen anser att det i de nya lagarna bör tydliggöras att ett personuppgiftsbiträde som går utanför sin befogenhet och behandlar personuppgifter för något annat ändamål än enligt sina instruktioner är personuppgiftsansvarig. I sådana fall kan personuppgiftsbiträdet bli skadeståndsskyldig på grund av den behandlingen.

11.5.4 Övriga skyldigheter för personuppgiftsbiträden

Regeringens förslag: Ett personuppgiftsbiträde ska ha samma skyldigheter som en personuppgiftsansvarig att begränsa tillgången till personuppgifter och vidta säkerhetsåtgärder.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna yttrar sig inte särskilt över utredningens förslag.

Skälen för regeringens förslag: Enligt gällande rätt är ett personuppgiftsbiträde skyldigt att vidta vissa säkerhetsåtgärder. Försvarsmakten och Försvarets radioanstalt ska förvissa sig om att det personuppgiftsbiträde som myndigheten anlitar kan genomföra de säkerhetsåtgärder som måste vidtas och se till att personuppgiftsbiträdet verkligen vidtar åtgärderna (3 kap. 1 och 2 § FM-PuL och FRA-PuL). Personuppgiftsbiträden är alltså enligt nuvarande ordning skyldiga att vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. I enlighet med utredningens förslag bör dessa skyldigheter även komma till uttryck i de nya lagarna, liksom skyldigheten att begränsa tillgången till personuppgifter genom exempelvis behörighetstilldelning.

12 Enskildas rättigheter

12.1 Rätten till information

12.1.1 Information som ska göras allmänt tillgänglig

Regeringens förslag: Försvarsmakten och Försvarets radioanstalt ska göra viss information allmänt tillgänglig för den registrerade. Bland annat ska kategorier av ändamål för behandlingen göras tillgängliga.

Information som ska göras allmänt tillgänglig ska lämnas utan avgift.

Utredningens förslag överensstämmer i huvudsak med regeringens. Enligt utredningens förslag ska ändamålen med behandlingen göras tillgänglig.

Remissinstanserna tillstyrker eller invänder inte mot utredningens förslag.

Skälen för regeringens förslag: Försvarsmakten och Försvarets radioanstalt bör hålla viss information allmänt tillgänglig för den registrerade. Sådan information bör omfatta myndighetens identitet och kontaktuppgifter, uppgifter om dataskyddsombudet, kategorier av ändamål med behandlingen, rätten att begära att få information om behandling av personuppgifter och att få ta del av dem, samt rätten att begära rättelse, radering eller begränsning av behandlingen.

I kravet på att informationen ska vara allmänt tillgänglig ligger att allmänheten i princip ska ha möjlighet att kunna ta del av informationen när den önskar. Informationen kan t.ex. publiceras på myndigheternas webbplatser eller finnas i en broschyr eller annan informationsskrift.

Det bör 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.

Regeringen anser att det av de nya lagarna bör framgå att den information som görs allmänt tillgänglig ska vara avgiftsfri.

12.1.2 Enskildas rätt till personrelaterad information

Regeringens förslag: Försvarsmakten och Försvarets radioanstalt är skyldiga att en gång per kalenderår till den som begär det lämna skriftligt besked om huruvida personuppgifter som rör honom eller henne behandlas. Om sådana uppgifter behandlas ska sökanden få del av dem och få viss skriftlig information om behandlingen.

Ett 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.

Information 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.

Information som ska lämnas efter begäran från den registrerade ska lämnas utan avgift en gång per kalenderår.

Om Försvarsmakten samlar in personuppgifter från den som uppgifterna avser ska myndigheten i samband med det lämna viss information om behandlingen. Informationen ska lämnas utan avgift.

Utredningens förslag överensstämmer i sak med regeringens.

Remissinstanserna: *Försvarsmakten* föreslår ett förtydligande av utredningens förslag då det enligt myndigheten inte är möjligt att få del av handlingarna i vilka personuppgifterna behandlas genom en begäran om personrelaterad information. *Försvarets radioanstalt* avstyrker utredningens förslag om enskildas möjlighet till registerutdrag i försvarsunderrättelse- och utvecklingsverksamheten. *Totalförsvarets rekryteringsmyndighet* uppmärksammar att den registrerade har rätt att enligt EU:s dataskyddsförordning begära information och få tillgång till de personuppgifter som den personuppgiftsansvarige behandlar ett obegränsat antal gånger per år, men bedömer samtidigt att utredningens förslag inte torde medföra några större verkningar för den enskilde.

Skälen för regeringens förslag

Information som Försvarsmakten ska lämna om uppgifterna samlas in från den registrerade

När Försvarsmakten samlar in uppgifter om en person i den militära säkerhetstjänsten från den enskilde, ska myndigheten i samband med insamlingen självmant lämna information om behandlingen av uppgifterna (2 kap. 1 § FM-PuL). 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.

Av samma bestämmelse framgår att information inte behöver lämnas om sådant som den registrerade redan känner till. Det kan vara sådant som den registrerade 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 registrerade. Information

behöver då inte lämnas varje gång nya uppgifter samlas in, om den registrerade en gång har fått fullständig information och således redan känner till informationen. Bestämmelsen tillämpas huvudsakligen i samband med säkerhetsprövning enligt säkerhetsskyddslagen inför bl.a. anställning, uppdrag och tjänstgöring inom Försvarsmakten.

Förutom i den militära säkerhetstjänsten, kommer Försvarsmakten även inom verksamhetsområdena Sveriges försvar och säkerhet och internationellt försvars- och säkerhetssamarbete ibland att behandla personuppgifter som har lämnats av den enskilde själv. Som utredningen föreslår bör det i den nya lagen därför införas en bestämmelse som innebär att Försvarsmakten på eget initiativ ska lämna viss information om personuppgiftsbehandlingen i de fall uppgifterna samlas in från den som uppgifterna avser.

I enlighet med utredningens förslag bör det av den nya lagen framgå att den information som Försvarsmakten lämnar i dessa situationer ska vara avgiftsfri.

Information som ska lämnas efter begäran

Försvarsmakten och Försvarets radioanstalt är enligt gällande ordning 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 myndigheterna lämna skriftlig information om vilka uppgifter om den sökanden som behandlas, varifrån dessa uppgifter har hämtats, ändamålen med behandlingen och till vilka mottagare eller kategorier av mottagare som uppgifterna lämnas ut. En ansökan ska göras skriftligen och vara undertecknad av den sökande själv. Försvarsmakten och Försvarets radioanstalt ska lämna information till den sökande inom en månad efter det att ansökan gjordes. Om det finns särskilda skäl för det får informationen lämnas senast fyra månader efter det att ansökan gjordes (2 kap. 2 § FM-PuL och 2 kap. 1 § FRA-PuL).

Utredningen föreslår att motsvarande bestämmelser bör införas i de nya lagarna. Enligt utredningens förslag bör den skriftliga informationen även innehålla uppgifter om hur länge personuppgifterna får behandlas eller, om det inte är möjligt att ange, kriterierna för att fastställa det och rätten att begära rättelse, radering eller begränsning av behandling.

Försvarets radioanstalt avstyrker utredningens förslag, med hänvisning till att myndigheten efter bedömning av den sekretess som omgärdar försvarsunderrättelseverksamheten, hittills inte i något fall har lämnat ut någon personuppgift efter en enskilds begäran (rätten att begränsa rätten till information behandlas i avsnitt 12.2). Myndigheten framhåller även att skyddet av den enskildes integritet på ett bättre sätt säkerställs av den omfattande och oberoende statliga kontroll som finns på försvarsunderrättelseområdet.

Regeringen instämmer i att kontrollverksamheten är av väsentlig betydelse för värnandet av den enskildes integritet. Det betyder emellertid inte att den rätt till information som den enskilde har enligt nuvarande ordning bör utgå. Utredningens förslag i denna del bör därför genomföras.

Försvarsmakten föreslår ett förtydligande i förhållande till utredningens lagtextförslag då det enligt Försvarsmakten inte är möjligt att få del av handlingarna i vilka personuppgifterna behandlas genom en begäran om

personrelaterad information. Försvarsmakten framhåller att en enskild alltid har möjlighet att begära att få ta del av en allmän handling enligt 2 kap. tryckfrihetsförordningen. Regeringen, som inte anser att det finns skäl att justera bestämmelsen, konstaterar att det inte finns något som hindrar att den, som med stöd av personuppgiftsregleringen begär att få ta del av sina personuppgifter, får detta genom en kopia av den handling i vilka uppgifterna finns. Den personuppgiftsansvarige har dock ingen skyldighet att lämna ut en kopia av handlingen om sökandens rättigheter kan säkerställas på annat sätt, t.ex. genom en sammanställning av vilka personuppgifter som behandlas.

Som *Totalförsvarets rekryteringsmyndighet* uppmärksammar innebär förslaget en skillnad i förhållande till EU:s dataskyddsförordning när det gäller hur ofta den enskilde kan begära att få ta del av sina personuppgifter. Regeringen bedömer, i likhet med myndigheten, att det kan antas medföra verkningar av enbart begränsad betydelse för den enskilde. Enligt nuvarande ordning och utredningens förslag ska information som ska lämnas efter begäran från den registrerade lämnas utan avgift en gång per kalenderår. Utredningen föreslår även att de nya lagarna uttryckligen ska ge Försvarsmakten respektive Försvarets radioanstalt rätt att avslå en begäran från någon som begär information om personuppgifter oftare än en gång per kalenderår. Regeringen anser att detta redan på ett tillräckligt tydligt sätt följer av de föreslagna bestämmelserna om att Försvarsmakten och Försvarets radioanstalt är skyldiga att en gång per kalenderår på begäran lämna skriftligt besked om huruvida personuppgifter om en viss person behandlas. Utredningens förslag i denna del bör därför inte genomföras.

12.2 Rätten till information får begränsas

Regeringens förslag: Informationsskyldigheten gäller inte i den utsträckning sekretess hindrar att uppgifterna lämnas ut.

Om det finns grund för att begränsa informationen ska den personuppgiftsansvarige inte heller vara skyldig att lämna ut skälen för ett beslut om att begränsa informationen eller för ett beslut om en begäran om rättelse, radering eller begränsning av behandlingen.

Rätten att få del av personrelaterad information ska inte gälla personuppgifter i löpande text som inte har fått sin slutliga utformning när begäran gjordes eller som utgör en minnesanteckning eller liknande. Informationsskyldigheten ska dock gälla om uppgifterna

1. har lämnats till tredje part, med undantag för en myndighet som med stöd av författning utövar tillsyn, kontroll eller revision,
2. behandlas enbart för statistiska ändamål eller arkivändamål av allmänt intresse, eller
3. har behandlats under längre tid än ett år i löpande text som inte har fått sin slutliga utformning.

Utredningens förslag stämmer i huvudsak överens med regeringens. Utredningen föreslår inte något undantag för uppgifter som har lämnats till en myndighet som med stöd av författning utövar tillsyn, kontroll eller revision.

Remissinstanserna: *Försvarsmakten* anser att förslaget om att informationsskyldighet föreligger för uppgifter som behandlas enbart för vissa ändamål bör få motsvarande omfattning som enligt dataskyddslagen.

Skälen för regeringens förslag: Enskildas rätt till information enligt FM-PuL och FRA-PuL hos Försvarsmakten och Försvarets radioanstalt begränsas av bestämmelser om sekretess (2 kap. 4 § FM-PuL och 2 kap. 3 § FRA-PuL). Den informationsskyldighet som behandlas i avsnitt 12.1.2 bör därför, på motsvarande sätt som enligt nuvarande ordning, inte gälla i den utsträckning sekretess hindrar att uppgifterna lämnas ut till den som uppgifterna rör. Eftersom skälen för ett beslut om sekretess kan ge ledning om uppgifternas innehåll, bör 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 (se avsnitt 12.3).

Lagrådet anser att lagförslaget bör förtydligas i den del som avser begränsning av information med hänsyn till sekretess och föreslår en annan språklig utformning. Regeringen anser att utformningen enligt lagrådsremissens förslag är tydligare och lämpligare och därför bör stå kvar.

Enligt nuvarande ordning behöver information som har begärts av en enskild inte 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 (2 kap. 3 § FM-PuL och 2 kap. 2 § FRA-PuL). Som utredningen föreslår bör motsvarande bestämmelser införas i de nya lagarna. Tredje part är, enligt den föreslagna definitionen, någon annan än den registrerade, den personuppgiftsansvarige, dataskyddsombudet, personuppgiftsbiträdet och sådana personer som under den personuppgiftsansvariges eller personuppgiftsbiträdets direkta ansvar har rätt att behandla personuppgifter (se avsnitt 6.5).

Enligt utredningens förslag ska personuppgifter även lämnas ut om uppgifterna behandlas för enbart vetenskapliga, statistiska eller historiska ändamål, eller arkivändamål av allmänt intresse. *Försvarsmakten* hänvisar till motsvarande bestämmelse i dataskyddslagen som i denna del omfattar sådana personuppgifter som behandlas enbart för arkivändamål av allmänt intresse eller statistiska ändamål. Till skillnad från utredningens förslag omfattar dataskyddslagens bestämmelse således inte sådana personuppgifter som behandlas för vetenskapliga och historiska ändamål.

Regeringen anser att de nya lagarna i denna del inte bör avvika från vad som gäller enligt dataskyddslagen. I de fall som ett utkast eller en minnesanteckning endast används för statistiska ändamål eller för arkivändamål av allmänt intresse, bör således information om personuppgiftsbehandlingen kunna lämnas. Detta bör komma till uttryck i de nya lagarna.

Med mottagare avses den till vilken personuppgifter lämnas ut, med undantag av en myndighet som med stöd av författning utövar tillsyn, kontroll eller revision (se avsnitt 6.5). Det är därför lämpligt att i den

aktuella bestämmelsen klargöra att ett utlämnande av information till sådana myndigheter inte gör att undantaget upphör att gälla.

12.3 Rättelse, radering och begränsning av behandlingen

Regeringens förslag: Försvarsmakten och Försvarets radioanstalt ska på begäran av den registrerade snarast rätta, radera eller begränsa behandlingen av 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 registrerade 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. Den personuppgiftsansvarige ska inte heller vara skyldig att lämna ut skälen för beslut i fråga om begäran om rättelse, radering eller begränsning av behandlingen.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Flertalet remissinstanser, däribland *Försvarsmakten*, tillstyrker eller invänder inte mot utredningens förslag. *Försvarets radioanstalt* avstyrker utredningens förslag om enskildas möjlighet att begära rättelse, radering och begränsning av behandling av personuppgifter i myndighetens försvarsunderrättelse- och underrättelseverksamhet.

Skälen för regeringens förslag

Nuvarande ordning

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 FM-PuL respektive FRA-PuL eller föreskrifter som har meddelats med stöd av lagarna. 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 (2 kap. 5 § FM-PuL och 2 kap. 4 § FRA-PuL).

Med blockering avses en åtgärd som vidtas för att personuppgifter ska förses med information om att de inte ska lämnas ut till tredje man (annat än med stöd av offentlighetsprincipen) och om anledningen till det. Sådana personuppgifter får dock fortfarande behandlas av den personuppgiftsansvarige eller av personuppgiftsbiträden. Att en uppgift utplånas innebär att den förstörs så att den inte kan återskapas.

I EU:s dataskyddsförordning används inte orden blockering och utplåning.

Rätten att begära rättelse

Att en personuppgift rättas innebär att den ersätts eller kompletteras med riktiga uppgifter. Att de personuppgifter som behandlas är riktiga är av grundläggande betydelse både för myndigheternas verksamhet och för enskilda. På motsvarande sätt som enligt nuvarande ordning bör de nya lagarna, som utredningen föreslår, därför innehålla en bestämmelse om rätt för den registrerade att begära rättelse.

Skyldigheten för den personuppgiftsansvarige att på eget initiativ vidta åtgärder när det upptäcks att personuppgifter är felaktiga, ofullständiga eller inaktuella behandlas i avsnitt 8.1.2. Den personuppgiftsansvarige bör skyndsamt utreda frågan och, om det är motiverat, så fort som möjligt genomföra rättelse eller korrigering. Den information som finns tillgänglig för den personuppgiftsansvarige, bl.a. den information som framgår av begäran om rättelse, bör tas i beaktande, men vilka utredningsåtgärder som i övrigt bör vidtas av den personuppgiftsansvarige får bedömas i varje enskilt fall.

Felaktiga och ofullständiga uppgifter

Att en felaktig eller ofullständig personuppgift rättas eller kompletteras kan innebära att uppgiften ersätts av en annan uppgift som är objektivt sett riktig eller kompletteras med en uppgift om de riktiga förhållandena så att uppgiften blir fullständig i objektiv mening. Det kan vara fråga om t.ex. ett felaktigt namn eller att endast delar av ett namn har återgetts i en handling (jfr avsnitt 8.1.2). Det kan även vara fråga om något fel som har uppstått på grund av ett tekniskt förfarande. Det ska alltså röra sig om ett fel eller en ofullständighet på grund av något som inte förutsätter en bedömning.

Regeringen anser, i likhet med utredningen, att det i de nya lagarna bör införas bestämmelser om att den personuppgiftsansvarige på begäran ska rätta personuppgifter som rör den registrerade om de är felaktiga eller ofullständiga med hänsyn till ändamålet med behandlingen. Att den personuppgiftsansvarige ska ta hänsyn till ändamålet med behandlingen vid bedömningen av om felaktiga personuppgifter ska rättas är en nödvändig del av prövningen av om en personuppgift är felaktig.

Bestämmelserna bör inte innebära en rättighet för den registrerade att kräva att den personuppgiftsansvarige rättar inaktuella uppgifter. Däremot ska den personuppgiftsansvarige – om det är nödvändigt – på eget initiativ uppdatera uppgifter som är inaktuella. En felaktig personuppgift kan också rättas på så sätt att uppgiften tas bort utan att ersättas.

Rätten till radering

Radering motsvarar utplåning, och är det ord som används i EU:s dataskyddsförordning. På samma sätt som när det gäller rättelse bör radering kunna göras dels på den personuppgiftsansvariges eget initiativ, dels på begäran av den registrerade. Den personuppgiftsansvarige ska på eget initiativ vidta åtgärder om personuppgifter behandlas i strid med vissa bestämmelser i lagarna. I enlighet med utredningens förslag bör rätten för

enskilda att begära att den personuppgiftsansvarige ska radera uppgifterna regleras i de nya lagarna enligt följande.

Personuppgifter ska vara adekvata och relevanta. Fler personuppgifter än nödvändigt får inte behandlas och de får bara behandlas om det finns en rättslig grund och för särskilt angivna ändamål. Det ska även anges i vilken utsträckning som känsliga personuppgifter får behandlas och hur länge personuppgifter får behandlas.

Frågan om huruvida en personuppgift bör raderas får bedömas mot bakgrund av dessa bestämmelser. Vid bedömningen måste även 2 kap. tryckfrihetsförordningen och det arkivrättsliga regelverket beaktas.

Uppgifter i allmänna handlingar

En grundläggande princip i svensk rätt är att allmänheten ska ha insyn i det allmännas verksamhet. Enligt tryckfrihetsförordningen får grundläggande föreskrifter om hur allmänna handlingar ska bevaras samt om gallring och annat avhändande av sådana handlingar meddelas i lag (2 kap. 23 §). Sådana föreskrifter finns för närvarande i arkivlagen (1990:782), vilken kompletteras av arkivförordningen (1991:446) och föreskrifter som har meddelats av Riksarkivet. Många av myndigheternas handlingar är allmänna och omfattas därmed av offentlighetsprincipen. Arkivlagstiftningen har som utgångspunkt företräde framför personuppgiftslagstiftningen på så sätt att intresset av att bevara allmänna handlingar väger över skyddet för personlig integritet. Utrymmet för att radera uppgifter i allmänna handlingar begränsas därmed av arkivlagstiftningen. Eftersom radering av uppgifter innebär att personuppgifter tas bort från uppgiftssamlingar på ett sådant sätt att de inte kan återskapas, bör en sådan åtgärd bara vidtas om den är förenlig med arkivlagstiftningen. För att radera personuppgifter i allmänna handlingar krävs därför författningsstöd för gallring. Utrymmet för att radera personuppgifter i allmänna handlingar på grund av att personuppgifterna inte har behandlats författningsenligt framstår därför som begränsat (jfr bl.a. Myndighetsdatalag, SOU 2015:39 s. 529 och 573–574).

Begränsning ersätter blockering

I enlighet med utredningens förslag bör ordet begränsning användas i de nya lagarna som motsvarighet till det som enligt nuvarande ordning benämns blockering. Med blockering av personuppgifter avses 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. tryckfrihetsförordningen (1 kap. 4 § FM-PuL och FRA-PuL och 3 § personuppgiftslagen).

Blockerade personuppgifter får användas internt av den personuppgiftsansvarige och av personuppgiftsbiträdet, under förutsättning att det framgår att uppgifterna är spärrade och anledningen till åtgärden. Däremot får personuppgifterna inte lämnas ut till tredje man, förutom enligt 2 kap. tryckfrihetsförordningen (prop. 1997/98:44 s. 117).

Vad avses med begränsning av behandling?

Begränsning av behandling definieras i EU:s dataskyddsförordning som en markering av lagrade personuppgifter med syftet att begränsa behandlingen av dessa i framtiden. Om behandlingen av personuppgifter har begränsats i stället för att uppgifterna raderas, bör uppgifterna endast behandlas för det ändamål som förhindrade raderingen. Exempel på begränsning av behandling kan vara att personuppgifterna flyttas till ett annat databehandlingssystem, t.ex. ett system för arkivering, eller att uppgifterna görs otillgängliga med hjälp av tekniska medel. För att åtgärden ska bli effektiv bör behandlingen begränsas redan i samband med markeringen.

Begränsning om det bestrids att personuppgifterna är riktiga

Begränsning av behandlingen kan komma i fråga om den registrerade bestrider att personuppgifterna är riktiga, men det inte är möjligt att fastställa om så är fallet. En felaktig personuppgift ska rättas snarast efter det att den registrerade har begärt det. Om den personuppgiftsansvariges utredning om den omstridda personuppgiften inte kan slutföras tillräckligt snabbt bör behandlingen begränsas under utredningstiden. Uppgifterna får då inte behandlas av den personuppgiftsansvarige eller personuppgiftsbiträden annat än för det ändamål som föranledde begränsningen. Om det efter utredning visar sig att personuppgifterna är riktiga kan behandlingen av dem fortsätta som tidigare. Begränsningen bör då upphävas. Innan dess ska dock den registrerade underrättas om att begränsningen upphör. Skulle det visa sig att personuppgifterna är felaktiga ska den personuppgiftsansvarige rätta dem, varefter begränsningen kan upphöra.

Val av åtgärd

Förslaget om grundläggande krav på behandling av personuppgifter innebär att Försvarsmakten och Försvarets radioanstalt på eget initiativ ska korrigera felaktiga personuppgifter. Lagförslagen omfattar inte behandling av uppgifter om juridiska personer. Intresset av att de uppgifter som behandlas är riktiga gör sig dock även gällande i de fall uppgifterna inte avser fysiska personer.

Det är av väsentlig betydelse för den enskilde att Försvarsmakten och Försvarets radioanstalt rättar personuppgifter som behandlas felaktigt så att intrång i den personliga integriteten kan undvikas. Bedömningen av om en uppgift har behandlats felaktigt måste göras mot bakgrund av de bestämmelser som gäller för behandlingen.

Den personuppgiftsansvarige ska enligt förslaget vidta alla rimliga åtgärder för att rätta personuppgifter som är felaktiga eller ofullständiga och för att radera eller begränsa behandlingen av personuppgifter som har behandlats otillåtet. Enligt förarbetena till personuppgiftslagen väljer den personuppgiftsansvarige själv vilket alternativ som ska användas av rättelse, utplånande eller blockering (prop. 1997/98:44 s. 87). Som utredningen föreslår bör den personuppgiftsansvarige på motsvarande sätt enligt de nya lagarna själv avgöra om en viss personuppgift ska rättas eller raderas eller om behandlingen ska begränsas. Den personuppgiftsansvarige är därmed inte bunden till att endast pröva om den åtgärd som

begärs av den registrerade bör vidtas, utan kan välja en annan åtgärd om den är lämpligare.

En åtgärd måste alltid ha stöd i lagstiftningen. Det innebär bl.a. att det krävs författningsstöd för gallring för att en myndighet ska få radera uppgifter i en allmän handling.

Underrättelse till tredje part

Försvarsmakten och Försvarets radioanstalt ska enligt gällande rätt underrätta tredje man till vilken uppgifterna har lämnats ut om åtgärden att rätta, blockera eller utplåna en personuppgift, 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. Som utredningen föreslår bör motsvarande gälla vid rättelse, radering eller begränsning enligt de nya lagarna.

I fråga om *Försvarets radioanstalts* invändning mot utredningens förslag gör regeringen samma bedömning som i avsnitt 12.1.2.

13 Tillsyn

13.1 Nuvarande ordning

Integritetsskyddsmyndigheten utövar tillsyn över Försvarsmaktens och Försvarets radioanstalts personuppgiftsbehandling som sker enligt FM-PuL och FRA-PuL, samt personuppgiftslagen. Härtill har Statens inspektion för försvarsunderrättelseverksamheten ett särskilt kompletterande kontrollansvar för den personuppgiftsbehandling som sker enligt FM-PuL och FRA-PuL.

Integritetsskyddsmyndigheten 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 Integritetsskyddsmyndigheten konstaterar att personuppgifter behandlas eller kan komma att behandlas på ett olagligt sätt, ska myndigheten genom påpekanden eller liknande förfaranden försöka åstadkomma rättelse. Integritetsskyddsmyndigheten 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 är ansvarig kontrollmyndighet för försvarsunderrättelseverksamhet som bedrivs enligt lagen om försvarsunderrättelseverksamhet och för signalspaning i sådan verksamhet enligt lagen om signalspaning i försvarsunderrättelse-verksamhet. Myndigheten har även till uppgift att granska behandlingen av uppgifter enligt FM-PuL och FRA-PuL (1–3 §§ förordningen [2009:969] med instruktion för Statens inspektion för försvarsunder-

rättelseverksamheten). Granskning sker genom inspektioner och andra undersökningar som är föranmälda (5 § första stycket). Statens inspektion för försvarsunderrättelseverksamheten har för sin granskning rätt att få tillgång till de uppgifter och den hjälp som myndigheten begär av den granskade myndigheten (6 §). Om Statens inspektion för försvarsunderrättelseverksamheten finner något att anmärka på får den lämna synpunkter och förslag på hur bristerna bör avhjälpas. Om det behövs, ska myndigheten också lämna dessa synpunkter och förslag om åtgärder till regeringen (5 § andra stycket).

I fråga om Försvarets radioanstalts signalspaning i försvarsunderrättelseverksamhet har Statens inspektion för försvarsunderrättelseverksamheten ett särskilt kontrollansvar för den verksamhet som bedrivs enligt lagstiftningen om signalspaning i försvarsunderrättelseverksamhet. Kontrollen ska särskilt avse granskning av sökbegrepp, förstöring av uppgifter samt rapportering enligt vad som närmare framgår av lagen (10 § lagen om signalspaning i försvarsunderrättelseverksamhet).

Statens inspektion för försvarsunderrättelseverksamheten får besluta att viss inhämtning ska upphöra eller att upptagning eller uppteckning av Försvarets radioanstalt inhämtade uppgifter ska förstöras, om det vid kontroll framkommer att inhämtningen inte är förenlig med tillstånd som har meddelats enligt lagen om signalspaning i försvarsunderrättelseverksamhet. Statens inspektion för försvarsunderrättelseverksamheten ska vidare, på begäran av en enskild, kontrollera om hans eller hennes meddelanden har inhämtats i samband med signalspaning enligt lagen och, om så är fallet, huruvida inhämtningen och behandlingen av inhämtade uppgifter har skett i enlighet med lagen. Myndigheten ska underrätta den enskilde om att kontrollen har utförts (jfr 10 a § lagen om signalspaning i försvarsunderrättelseverksamhet).

Om Statens inspektion för försvarsunderrättelseverksamheten upptäcker brott ska det anmälas till Åklagarmyndigheten och om nämnden finner något som kan leda till skadeståndsansvar för staten ska det anmälas till Justitiekanslern. Finner Statens inspektion för försvarsunderrättelseverksamheten omständigheter som Integritetsskyddsmyndigheten bör uppmärksammas på, ska det anmälas till Integritetsskyddsmyndigheten (15 § förordningen med instruktion för Statens inspektion för försvarsunderrättelseverksamheten).

Riksdagens ombudsmän (JO) och Justitiekanslern utövar tillsyn över hur lagar och andra föreskrifter tillämpas i offentlig verksamhet. Deras tillsyn omfattar därmed även behandlingen av personuppgifter och skyddet av enskildas personliga integritet vid sådan behandling. Både JO och Justitiekanslern är extraordinära tillsynsorgan.

13.2 Former för tillsyn till skydd för den personliga integriteten

Regeringens förslag: Den myndighet som regeringen bestämmer ska utöva tillsyn över Försvarsmaktens och Försvarets radioanstalts behandling av personuppgifter enligt de föreslagna lagarna, enligt föreskrifter som har meddelats i anslutning till lagarna och enligt beslut med stöd av lagarna.

Tillsynsmyndigheten ska, när det är motiverat, ge råd och stöd till Försvarsmakten respektive Försvarets radioanstalt och personuppgiftsbiträden i frågor som gäller deras skyldigheter enligt lag eller annan författning.

Utredningens förslag överensstämmer i huvudsak med regeringens. Utredningens förslag omfattar inte personuppgiftsbiträden.

Remissinstanserna invänder inte mot utredningens förslag.

Skälen för regeringens förslag: Enligt FM-PuL och FRA-PuL ska den myndighet som regeringen bestämmer utöva tillsyn över Försvarsmaktens och Försvarets radioanstalts behandling av personuppgifter enligt respektive lag (5 kap. 1 §). I de förordningar som ansluter till FM-PuL och FRA-PuL anges Integritetsskyddsmyndigheten som ansvarig tillsynsmyndighet. Detsamma bör gälla även enligt det nya regelverket. Statens inspektion för försvarsunderrättelseverksamhetens kompletterande kontrollansvar för den personuppgiftsbehandling som görs inom Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst och Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet bör inte heller ändras.

En central arbetsuppgift för tillsynsmyndigheten är att på eget initiativ eller på begäran ge information eller råd till olika aktörer om regler som styr behandlingen av personuppgifter. Regeringen noterar att det tidigare framgick av 1 § förordningen (2007:975) med instruktion för dåvarande Datainspektionen (numera Integritetsskyddsmyndigheten) att Datainspektionen bl.a. särskilt skulle inrikta sin verksamhet på att informera om gällande regler och ge råd och hjälp åt personuppgiftsombud. Denna uppgift togs bort i samband med att brottsdatalagen trädde i kraft den 1 augusti 2018 som ett led i arbetet med att ge tillsynsmyndigheten ökad självständighet i förhållande till regeringen (prop. 2017/18:232 s. 273–275). Regeringen fann emellertid att det inte finns något hinder mot att i lag ange råd och stöd till personuppgiftsansvariga och personuppgiftsbiträden som en uppgift för tillsynsmyndigheten bland flera, så länge regleringen inte innebär att den viktas högre eller lägre än någon av de andra uppgifterna som tillsynsmyndigheten har. En sådan bestämmelse finns i brottsdatalagen och i lagen om Säkerhetspolisens behandling av personuppgifter. Även de föreslagna bestämmelserna bör på samma sätt ge tydligt uttryck för att tillsynsmyndigheten själv avgör när råd och stöd kan vara motiverat. Tillsynsmyndigheten ska således, när det är motiverat, ge råd och stöd till Försvarsmakten och Försvarets radioanstalt i frågor som gäller myndigheternas skyldigheter enligt lag eller annan författning.

Som utvecklas i avsnitt 13.3 omfattar tillsynsmyndighetens tillsyn även myndigheternas personuppgiftsbiträden. Regeringen föreslår därför att

tillsynsmyndighetens uppgift att vid behov lämna råd och stöd även ska avse personuppgiftsbiträden till Försvarsmakten och Försvarets radioanstalt.

Dataskyddsombuden vid Försvarsmakten och Försvarets radioanstalt kommer även fortsättningsvis att vid behov inhämta råd och stöd från tillsynsmyndigheten i olika frågor. I den utsträckning dataskyddsombud har behov av råd och stöd från tillsynsmyndigheten bör myndigheten tillgodose det behovet på samma sätt som enligt nuvarande ordning.

13.3 Tillsynsmyndighetens befogenheter

13.3.1 Undersökningsbefogenheter

Regeringens förslag: 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. den hjälp och annan information som behövs för tillsynen.

Utredningens förslag överensstämmer i sak med regeringens.

Remissinstanserna yttrar sig inte över utredningens förslag.

Skälen för regeringens förslag: Tillsynsmyndighetens funktion, uppgifter och undersökningsbefogenheter regleras för närvarande i 5 kap. 2 § FM-PuL och FRA-PuL. Enligt bestämmelserna har tillsynsmyndigheten 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.

Regeringen anser att de nya lagarna, med några tillägg, bör innehålla motsvarande reglering. Det bör således av de nya lagarna framgå att tillsynsmyndigheten på begäran ska få tillgång till personuppgifter som behandlas samt 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. Det bör också framgå att tillsynsmyndigheten ska få den hjälp och annan information som behövs för tillsynen.

13.3.2 Förebyggande befogenheter

Regeringens förslag: 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 motverka den risken.

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

Utredningens förslag överensstämmer med regeringens.
Remissinstanserna yttrar sig inte särskilt över utredningens förslag.

Skälen för regeringens förslag

Gällande bestämmelser

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 (5 kap. 3 § FM-PuL och FRA-PuL).

Råd och stöd

En viktig uppgift för tillsynsmyndigheten är att lämna råd till personuppgiftsansvariga och personuppgiftsbiträden om deras skyldigheter och att stödja deras strävanden att skapa författningsenliga och integritetssäkra lösningar. Inom ramen för det förebyggande arbetet bör tillsynsmyndigheten på olika sätt försöka förmå den som är ansvarig att vidta de åtgärder som behövs för att motverka risken för att behandling av personuppgifter kan komma att stå i strid med lag eller annan författning. Medlen för det bör främst vara muntliga eller skriftliga råd, rekommendationer och påpekanden som inte är tvingande. Vilka åtgärder som bör vidtas bör i första hand lämnas åt den personuppgiftsansvarige eller personuppgiftsbiträdet att avgöra. I många fall kan det enligt regeringen antas vara tillräckligt att tillsynsmyndigheten upplyser om på vilket sätt personuppgiftsbehandlingen riskerar att vara oförenlig med regelverket.

Regeringen föreslår att detta kommer till uttryck i de nya lagarna i enlighet med utredningens förslag.

Varning

Tillsynsmyndigheten bör, som utredningen föreslår, kunna besluta om en varning till Försvarsmakten, Försvarets radioanstalt eller personuppgiftsbiträden för att planerade behandlingar sannolikt kommer att strida mot regelverket för personuppgiftsbehandling. Regeringen anser att denna möjlighet, som är ny, utgör ett lämpligt komplement till de förebyggande åtgärder som finns enligt nuvarande ordning.

Beslut om varning bör kunna användas av tillsynsmyndigheten för att i ett enskilt fall markera allvaret i en situation och försöka förmå den

personuppgiftsansvarige eller personuppgiftsbiträdet att ändra sig i fråga om planerad behandling. På så sätt kan det undvikas att behandling som inte är förenlig med regelverket påbörjas. Varning bör emellertid även kunna användas om pågående behandling riskerar att strida mot lag eller annan författning. Att besluta om varning bör som regel bli aktuellt först om tillsynsmyndigheten bedömer att den inte på annat sätt kan förmå den personuppgiftsansvarige eller personuppgiftsbiträdet att följa regelverket.

Ett beslut om varning bör enligt regeringens mening fungera som en tidig signal för den personuppgiftsansvarige om brister i en planerad eller pågående behandling av personuppgifter. Ett beslut om varning bör inte vara tvingande men bör ändå kunna ses som ett steg på vägen mot ett föreläggande, om åtgärder inte vidtas.

Ett beslut om varning bör vara skriftligt och tydligt ange på vilket sätt behandlingen riskerar att strida mot regelverket.

13.3.3 Korrigerande befogenheter

Regeringens förslag: Om tillsynsmyndigheten konstaterar att personuppgifter behandlas i strid med lag eller annan författning, eller att Försvarsmakten eller Försvarets radioanstalt eller ett personuppgiftsbiträde på annat sätt inte fullgör sina skyldigheter, får tillsynsmyndigheten

1. genom råd, rekommendationer eller påpekanden försöka förmå Försvarsmakten eller Försvarets radioanstalt eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsenlig eller för att fullgöra andra skyldigheter, eller
2. besluta att förelägga Försvarsmakten eller Försvarets radioanstalt eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsenlig eller för att fullgöra andra skyldigheter.

Av ett beslut om föreläggande ska det framgå när föreläggandet senast ska ha följts, och om det är lämpligt, vilka åtgärder som ska vidtas.

Utredningens förslag överensstämmer i huvudsak med regeringens.

Remissinstanserna: *Datainspektionen* anser att det ska finnas en möjlighet för tillsynsmyndigheten att kunna besluta om förbud mot en viss behandling av personuppgifter. Datainspektionen efterfrågar också ett tydliggörande av utredningens förslag om att tillsynsmyndigheten ska få besluta om förelägganden. Övriga remissinstanser yttrar sig inte särskilt över utredningens förslag.

Skälen för regeringens förslag

Gällande bestämmelser

Tillsynsmyndigheten får hos förvaltningsrätten inom vars domkrets tillsynsmyndigheten är belägen ansöka om att sådana personuppgifter som har behandlats på ett olagligt sätt ska utplånas. Beslut om utplånande får inte meddelas om det är oskäligt (5 kap. 4 § FM-PuL och FRA-PuL).

Vilka åtgärder kan komma i fråga?

Om tillsynsmyndigheten konstaterar att den personuppgiftsansvarige eller personuppgiftsbiträdet inte uppfyller kraven på författningsenlig personuppgiftsbehandling bör myndigheten uppmana den ansvarige och biträdet att fullgöra sina skyldigheter. Det kan göras genom vissa av de åtgärder som typisk sett används i det förebyggande arbetet, nämligen råd, rekommendationer eller påpekanden. Om den personuppgiftsansvarige eller personuppgiftsbiträdet vidtar de åtgärder som krävs så snart tillsynsmyndigheten väcker en fråga kan fortsatt dialog vara tillräcklig. Tillsynsmyndigheten behöver emellertid också ha möjlighet att få den personuppgiftsansvarige eller personuppgiftsbiträdet att fullgöra sina skyldigheter. Medlet för detta bör enligt regeringen vara beslut om förelägganden.

Beslut om förelägganden

Tillsynsmyndigheten bör, som utredningen föreslår, kunna besluta om förelägganden som innebär en skyldighet för den som är föremål för tillsynen att vidta vissa åtgärder för att göra personuppgiftsbehandlingen författningsenlig. När det gäller sådana åtgärder kan det i vissa fall vara lämpligt att tillsynsmyndigheten i beslutet om föreläggande anger vilken åtgärd som ska vidtas. I andra fall är det dock lämpligare att den som ska fullgöra skyldigheten själv avgör vad som bör göras för att behandlingen ska bli författningsenlig. Det kan t.ex. vara fråga om vilka tekniska åtgärder som bör vidtas eller vilka säkerhetslösningar som bör väljas. Tillsynsmyndigheten bör därför ange vilken åtgärd som ska vidtas enbart i de fall som detta är lämpligt. Däremot ska det alltid framgå av ett beslut om föreläggande när föreläggandet senast ska ha följts.

Datainspektionen efterfrågar ett tydliggörande avseende tillsynsmyndighetens möjligheter att besluta om föreläggande som en korrigerande befogenhet. Regeringen, som noterar att en motsvarande bestämmelse bl.a. finns i lagen om Säkerhetspolisens behandling av personuppgifter, ser inte behov av att i de nya lagarna närmare reglera vad ett beslut om föreläggandet får avse. Rättelse, radering och begränsning av behandlingen utgör dock exempel på åtgärder som tillsynsmyndigheten kan besluta ska vidtas. Om tillsynsmyndigheten överväger att besluta att förelägga tillsynsobjektet att radera en uppgift måste myndigheten dock beakta att åtgärden inte får stå i strid med annan lagstiftning, t.ex. 2 kap. tryckfrihetsförordningen.

Tillsynsmyndigheten bör inte bara kunna besluta om förelägganden för att säkerställa att personuppgiftsbehandling ska vara författningsenlig. Den bör även kunna besluta om förelägganden som tar sikte på att personuppgiftsansvariga och personuppgiftsbiträden ska fullgöra andra skyldigheter enligt det aktuella regelverket. Det kan t.ex. gälla att införa bättre säkerhetslösningar, fullgöra dokumentationsskyldighet eller att överlämna viss dokumentation eller ge tillträde till lokaler.

Tillsynsmyndigheten ska inte få förbjuda behandling av personuppgifter

Datainspektionen anser att det ska finnas en möjlighet för tillsynsmyndigheten att besluta om förbud mot en viss behandling av personuppgifter.

Regeringen noterar att EU:s dataskyddsförordning och viss annan dataskyddslagstiftning ger tillsynsmyndigheten befogenhet att förbjuda fortsatt behandling av personuppgifter även hos myndigheter. FM-PuL och FRA-PuL ger inte tillsynsmyndigheten en sådan befogenhet. På motsvarande sätt som anfördes i lagstiftningsärendet om Totalförsvarets plikt- och prövningsverk (Totalförsvarsdatalag – personuppgiftsbehandling vid Totalförsvarets rekryteringsmyndighet, prop. 2019/20:51 s. 65–66) anser regeringen att Försvarsmaktens och Försvarets radioanstalts behandling av personuppgifter är av sådan betydelse för försvaret av Sverige och rikets säkerhet att en förbudsmöjlighet inte är rimlig och därför inte bör införas.

Regeringen bedömer att de korrigerande befogenheter i form av bl.a. beslut om varning och förelägganden som tillsynsmyndigheten föreslås få är tillräckliga för att den ska kunna utföra sin tillsyn på ett effektivt sätt.

14 Sanktioner, skadestånd och rättsmedel

14.1 Ingen straffbestämmelse i de nya lagarna

Regeringens bedömning: Överträdelser av bestämmelserna om personuppgiftsbehandling bör inte vara straffsanktionerade utöver vad som gäller enligt brottsbalken.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna invänder inte mot utredningens bedömning.

Skälen för regeringens bedömning: Bestämmelser om straff för vissa gärningar i samband med personuppgiftshantering regleras särskilt i 6 kap. 2 § FM-PuL och FRA-PuL. Straffbestämmelserna omfattar den som uppsåtligen eller av grov oaktsamhet lämnar osann uppgift i information till den som personuppgiften rör eller till tillsynsmyndigheten, eller som behandlar känsliga uppgifter i strid med vad som gäller enligt de särskilda bestämmelserna för den behandlingen. Straffet är böter eller fängelse i högst sex månader, eller om brottet är grovt, fängelse i högst två år. I ringa fall döms inte till ansvar. Bestämmelserna om straff vid visst förfarande med personuppgifter har sitt ursprung i motsvarande bestämmelser i personuppgiftslagen. Dataskyddslagen innehåller inte någon straffbestämmelse.

Brottsbalken innehåller bestämmelser som kan innebära att vissa gärningar som innefattar personuppgiftsbehandling omfattas av straffansvar – såsom bestämmelserna om dataintrång (4 kap. 9 c § brottsbalken), kränkande fotografering (4 kap. 6 a § brottsbalken), olaga integritetsintrång (4 kap. 6 c § brottsbalken), förtal (5 kap. 1 § brottsbalken) och tjänstefel (20 kap. 1 § brottsbalken). Vidare innehåller lagen (1994:260) om offentlig anställning bestämmelser om disciplinansvar som kan aktualiseras om någon bryter mot bestämmelserna om personuppgiftsbehandling. Disciplinansvar förutsätter att den misstänkta gärningen inte ska anmälas till åtal eller, om den redan prövats

straffrättsligt, att den inte har ansetts vara något brott av annat skäl än bristande bevisning.

Kriminalisering som metod för att försöka hindra överträdelser av olika normer i samhället bör användas med försiktighet. Ett skäl till detta är att en alltför omfattande kriminalisering riskerar att undergräva straffsystemets brottsavhållande verkan, särskilt om rättsväsendet inte kan beivra alla brott på ett effektivt sätt. Ett annat skäl är att kriminalisering innebär påtagliga inskränkningar i medborgarnas valfrihet och ingripande tvångsåtgärder mot den som begår brott. När det gäller överträdelser av dataskyddsregleringen utgör straff inte en särskilt effektiv sanktion vid överträdelser av dataskyddsregleringen, eftersom det i många fall är svårt att identifiera en fysisk person som ansvarig för överträdelsen samt att leda i bevis att denne haft uppsåt eller varit oaktsam på det sätt som krävs för straffbarhet.

Mot denna bakgrund anser regeringen att de nya lagarna inte bör innehålla särskilda bestämmelser om straff.

14.2 Ingen möjlighet att ta ut sanktionsavgift

Regeringens bedömning: Det bör inte tas in bestämmelser om sanktionsavgift i de nya lagarna.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: *Försvarsmakten* och *Försvarets radioanstalt* ställer sig bakom utredningens bedömning. *Datainspektionen* anser att sanktionsavgifter fyller en viktig funktion för att säkerställa regelefterlevnad. *TCO* anser att tillsynsmyndigheten ska kunna besluta om sanktionsavgifter.

Skälen för regeringens bedömning: Enligt dataskyddslagen får tillsynsmyndigheten ta ut administrativa sanktionsavgifter av myndigheter vid vissa överträdelser av dataskyddsförordningen. Bestämmelsen reglerar även avgiftens storlek (6 kap. 2 §). I prop. 2017/18:105 utvecklar regeringen skälen för att tillsynsmyndigheten ska ha möjlighet att ta ut administrativa sanktionsavgifter från myndigheter (s. 139–142). Lagen om Säkerhetspolisens behandling av personuppgifter innehåller inte några bestämmelser om sanktionsavgifter (prop. 2018/19:163 s. 182–184).

De krav på sanktionsavgifter som unionsrätten ställer gäller inte för sådan behandling av personuppgifter som regleras i den lagstiftning som nu är aktuell. Dataskyddskonventionen 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. Regeringen föreslår inte någon ändring i detta avseende. Vidare kan straffrättsligt ansvar utkrävas enligt brottsbalken i enlighet med vad som redovisas i avsnitt 14.1. Utöver Integritetsskyddsmyndighetens tillsynsverksamhet granskar Statens inspektion för försvarsunderrättelseverksamheten behandlingen av personuppgifter enligt FM-PuL och FRA-PuL.

När det gäller Försvarets radioanstalts signalspaning i försvarsunderrättelseverksamhet finns även bestämmelser som är av intresse i lagen om signalspaning i försvarsunderrättelseverksamheten. Signalspaningsmyndigheten (Försvarets radioanstalt) ska ansöka om tillstånd hos Försvarsunderrättelsedomstolen för signalspaning enligt lagen (4 a §). Kontrollmyndigheten (Statens inspektion för försvarsunderrättelseverksamheten) 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 §).

Som *Datainspektionen* uppmärksammar kan sanktionsavgift i många fall fylla en viktig funktion för att säkerställa regelefterlevnad. Till skillnad från *TCO* anser regeringen dock inte att det finns skäl att överväga en sådan ordning för tillsyn enligt de nya lagarna. Mot bakgrund av den tillsyn, kontroll och granskning som gäller för de verksamheter som de nya lagarna omfattar, med tillhörande sanktionsmöjligheter, bedömer regeringen att dataskyddskonventionens krav på lämpliga sanktioner och rättsmedel är uppfyllda genom utredningens förslag.

14.3 Skadestånd

14.3.1 Det allmännas skadeståndsansvar

Enligt 3 kap. 2 § skadeståndslagen (1972:207) ska staten eller en kommun ersätta personskada, sakskada eller ren förmögenhetsskada som vållas genom fel eller försummelse vid myndighetsutövning i verksamhet för vars fullgörande staten eller kommunen svarar. Ersättningsskyldigheten omfattar även ideell skada på grund av att någon genom fel eller försummelse vid myndighetsutövning kränkts på det sätt som anges i 2 kap. 3 § samma lag.

I 2 kap. 3 § skadeståndslagen anges att den som allvarligt kränker någon annan genom brott som innefattar ett angrepp mot dennes person, frihet, frid eller ära ska ersätta den skada som kränkningen innebär. Ideellt skadestånd för att den personliga integriteten har kränkts, dvs. en skada av icke-ekonomisk natur, förutsätter alltså att kränkningen har orsakats genom brott. Det krävs också att kränkningen är allvarlig.

Ersättning för kränkning med stöd av 3 kap. 2 § jämförd med 2 kap. 3 § skadeståndslagen förutsätter att kränkningen har orsakats vid myndighetsutövning. Om det inte är fråga om myndighetsutövning kan skadestånd ändå utgå enligt 3 kap. 1 § skadeståndslagen för skada som vållats av arbetstagare. Det förutsätter att kränkningen har orsakats av att den anställde har begått brott i tjänsteutövningen.

Enligt 3 kap. 4 § skadeståndslagen ska staten eller en kommun ersätta personskada, sakskada, ren förmögenhetsskada och skada på grund av att någon kränks på sätt som anges i 2 kap. 3 §, om skadan uppkommit till följd av att den skadelidandes rättigheter enligt Europakonventionen har överträtts från statens eller kommunens sida, och annan ideell skada som uppkommit till följd av en sådan rättighetsöverträdelse. Enligt bestämmelsen ska skadestånd endast utges i den utsträckning det är nödvändigt för att gottgöra överträdelsen.

Den som anser att han eller hon har orsakats skada av det allmänna kan väcka talan mot staten eller en kommun vid allmän domstol. Saken prövas då som tvistemål.

Enligt förordningen (1995:1301) om handläggning av skadeståndsanspråk mot staten kan en skadelidande dessutom få ett skadeståndskrav mot staten prövat inom ramen för statens frivilliga skadereglering. Med det avses skadereglering som företrädelsevis sker hos Justitiekanslern, men som även i viss omfattning kan förekomma hos andra myndigheter. Enligt förordningen kan den enskilde i ett formlöst och kostnadsfritt förfarande vända sig direkt till en myndighet och få ett besked i frågan om huruvida staten är skadeståndsskyldig. Det är ett särskilt snabbt och effektivt sätt att komma i åtnjutande av det rättsmedel som rätten till skadestånd innebär. Vid ett negativt besked har den enskilde kvar möjligheten att vända sig till domstol för att få saken prövad. Justitiekanslerns inställning är inte bindande för domstolarna eller för den enskilde.

Enligt förordningen kan Justitiekanslern bl.a. handlägga anspråk som grundas på 3 kap. 1 eller 2 § skadeståndslagen eller skadeståndsregler i vissa särskilt angivna författningar, t.ex. FM-PuL och FRA-PuL.

14.3.2 Skadeståndsansvar för den personuppgiftsansvarige

Regeringens förslag: Den personuppgiftsansvarige ska ersätta den registrerade för den skada och kränkning av den personliga integriteten som behandling av personuppgiften i strid med de nya lagarna, föreskrifter som har meddelats i anslutning till lagarna eller beslut med stöd av dem, har orsakat.

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

Utredningens förslag överensstämmer i huvudsak med regeringens.
Remissinstanserna yttrar sig inte särskilt över utredningens förslag.

Skälen för regeringens förslag

Nuvarande reglering

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.

Den personuppgiftsansvarige är ersättningsskyldig gentemot den vars personuppgifter har behandlats så snart en sådan behandling har skett i strid med någon bestämmelse i lagen, såsom t.ex. någon av bestämmelserna om grundläggande krav på personuppgiftsbehandlingen, eller föreskrifter som har meddelats med stöd av lagen. Det krävs inte att

den personuppgiftsansvarige haft uppsåt att handla i strid med lagen eller varit oaktsam. Ersättningsskyldighet föreligger alltså även när den personuppgiftsansvarige bevisligen är oskyldig till felet. Skälet till denna stränga reglering är bestämmelsens syfte att skydda människors integritet.

Även personuppgiftslagen innehåller en bestämmelse om skadestånd med möjlighet till jämkning (48 §).

Det bör införas bestämmelser om skadeståndsskyldighet i de nya lagarna

Det bör i de nya lagarna införas motsvarande bestämmelser om skadeståndsansvar som gäller enligt nuvarande ordning, med ett tydliggörande om att det är den personuppgiftsansvarige som ska ersätta den drabbade vid felaktig behandling av personuppgifter enligt de nya lagarna, föreskrifter som har meddelats i anslutning till lagarna eller beslut med stöd av dem.

Enligt 3 § förordningen om handläggning av skadeståndsanspråk mot staten handlägger Justitiekanslern anspråk på ersättning enligt nuvarande 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 till Justitiekanslern för vidare hantering och beslut. För det fall att 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.

På samma sätt som gäller enligt nuvarande ordning bör det av bestämmelserna i de nya lagarna framgå att det finns en möjlighet att jämka skadeståndet om den personuppgiftsansvarige kan visa att felet inte berodde på myndigheten.

Skadeståndets omfattning och beräkningen av ersättningen

Rätten till personlig integritet är en immateriell rättighet. Den personuppgiftsansvarige är därför ersättningsskyldig inte bara för ekonomisk skada utan även för ideell skada. Den enskilde har alltså förutom rätt till ersättning för personskada, sakskada och ren förmögenhetsskada, rätt till ekonomisk kompensation för kränkningen. Det är bara skada eller kränkning som behandlingen har fört med sig som ska ersättas. Orsakssambandet ska vara adekvat.

I enlighet med gällande ordning bör ersättningen för kränkningen uppskattas efter skälighet, mot bakgrund av samtliga omständigheter. Det som kan ha betydelse är bl.a. att personuppgifter spridits eller att det har funnits risk för otillbörlig spridning av integritetskänsliga eller felaktiga personuppgifter. En annan omständighet kan vara att den registrerade drabbats av beslut eller andra åtgärder som fått eller kunnat få negativa konsekvenser för honom eller henne. Om den registrerade har lämnat oriktig eller ofullständig information till den personuppgiftsansvarige, kan även detta ha betydelse vid beräkningen.

Bestämmelserna om skadestånd i de nya lagarna utgör sådana särskilda föreskrifter om skadestånd som enligt 1 kap. 1 § skadeståndslagen tillämpas i stället för de allmänna bestämmelserna i den lagen. Om en viss ersättningsfråga inte behandlas i de nya lagarna – t.ex. hur ersättningen för en personskada eller sakskada ska beräknas (5 kap. skadeståndslagen) eller hur ansvaret ska fördelas när flera är skadeståndsskyldiga (6 kap. 4 § skadeståndslagen) – tillämpas de allmänna bestämmelserna i skadeståndslagen.

14.4 Överklagande

14.4.1 Överklagande av Försvarsmaktens och Försvarets radioanstalts beslut

Regeringens förslag: Försvarsmaktens och Försvarets radioanstalts beslut att inte lämna information efter begäran av en enskild och beslut i fråga om rättelse, radering eller begränsning av behandlingen eller underrättelse till tredje part, får överklagas till allmän förvaltningsdomstol.

Vid överklagande till kammarrätten ska det krävas prövningstillstånd.

Några andra beslut än de som uttryckligen anges i lagarna ska inte få överklagas.

Utredningens förslag överensstämmer i huvudsak med regeringens. Utredningens föreslår även en upplysningsbestämmelse om att kammarrätt är rätt forum för överklaganden av beslut som rör prövning enligt offentlighets- och sekretesslagen.

Remissinstanserna yttrar sig inte särskilt över utredningens förslag.

Skälen för regeringens förslag

Vilka beslut ska kunna överklagas?

Försvarsmaktens beslut om information som ska lämnas om uppgifterna samlas in från den som uppgifterna avser samt, efter begäran, Försvarsmaktens och Försvarets radioanstalts beslut om rättelse och underrättelse till tredje man får överklagas hos allmän förvaltningsdomstol. Andra beslut enligt respektive lag får inte överklagas. Prövningstillstånd krävs vid överklagande till kammarrätten (6 kap. 3 § FM-PuL och FRA-PuL).

De bestämmelser i FM-PuL och FRA-PuL som ger enskilda rätt till information efter ansökan samt rättelse och underrättelse till tredje part, föreslås med vissa justeringar och tillägg, införas även i de nya lagarna (jfr avsnitten 12.1.2, 12.2 och 12.3). Försvarsmaktens och Försvarets radioanstalts beslut i dessa frågor bör därför kunna överklagas till allmän förvaltningsdomstol på samma sätt som enligt FM-PuL och FRA-PuL. Även Försvarsmaktens och Försvarets radioanstalts beslut om radering och begränsning av behandlingen av personuppgifter bör kunna överklagas till allmän förvaltningsdomstol, med krav på prövningstillstånd vid överklagande till kammarrätten (jfr avsnitt 12.3).

På motsvarande sätt som enligt nuvarande ordning bör det av de nya lagarna framgå att andra beslut än de som anges inte får överklagas.

En upplysningsbestämmelse om överklagandeinstans för beslut som rör prövning enligt offentlighets- och sekretesslagen bör inte införas

Utredningen föreslår, med hänvisning till Högsta förvaltningsdomstolens avgörande som refereras i HFD 2014 ref. 55, att det i de nya lagarna ska föras in en upplysningsbestämmelse om att kammarrätt är rätt forum för överklaganden av beslut som rör prövning enligt offentlighets- och sekretesslagen. Regeringen vill understryka vikten av att överklaganden ges in till rätt instans, men anser inte att det finns behov av särskilda upplysningsbestämmelser om detta.

14.4.2 Överklagande av tillsynsmyndighetens beslut

Regeringens förslag: Tillsynsmyndighetens beslut om föreläggande enligt de nya lagarna ska få överklagas till allmän förvaltningsdomstol. När ett beslut överklagas är tillsynsmyndigheten motpart i domstolen.

Vid överklagande till kammarrätten ska det krävas prövningstillstånd.

Utredningen lämnar inte något förslag i denna del.

Remissinstanserna: *Datainspektionen* anser att myndighetens beslut ska kunna överklagas och att det särskilt bör anges i lagarna vad som går att överklaga.

Skälen för regeringens förslag

En överklagandebestämmelse bör tas in i den nya lagen

Enligt 42 § förvaltningslagen får ett beslut överklagas av den som beslutet angår, om det har gått honom eller henne emot.

Om en myndighets befogenheter regleras i en författning bör det av samma författning framgå om och i så fall hur myndighetens beslut kan överklagas (jfr En modern och rättssäker förvaltning – ny förvaltningslag, prop. 2016/17:180 s. 254). En sådan ordning ger en samlad bild både av vilka befogenheter en myndighet har och hur den som blir föremål för myndighetens beslut kan angripa dem. Tillsynsmyndighetens befogenheter enligt de nya lagarna behandlas i avsnitt 13.3. Som *Datainspektionen* föreslår bör det av lagarna också tydligt framgå vilka av tillsynsmyndighetens beslut som ska kunna överklagas.

Regeringen föreslår att lagtexten utformas i enlighet med detta.

Vilka beslut ska få överklagas?

Tillsynsmyndighetens beslut om föreläggande enligt de nya lagarna bör få överklagas till allmän förvaltningsdomstol. Vidare bör det krävas prövningstillstånd vid överklagande till kammarrätten.

Tillsynsmyndighetens beslut om varning faller enligt regeringens bedömning inte inom tillämpningsområdet för artikel 6.1 i Europakonventionen om rätten till domstolsprövning (jfr avsnitt 13.3.2). Det har inte heller i övrigt framkommit skäl för att sådana beslut eller andra beslut av tillsynsmyndigheten än beslut om föreläggande bör kunna överklagas.

Av tydlighetsskäl bör det av överklagandebestämmelsen även framgå att tillsynsmyndigheten har ställning som motpart i domstolen när ett beslut överklagas (jfr 7 kap. 3 § första stycket dataskyddslagen).

15 Ändringar i lagen om signalspaning i försvarsunderrättelseverksamhet

15.1 Signalspaning vid internationellt samarbete

Regeringens förslag: Det ska framgå av lagen om signalspaning i försvarsunderrättelseverksamhet att Försvarets radioanstalt under vissa villkor får bedriva signalspaning om det är nödvändigt inom ramen för myndighetens internationella samarbete i försvarsunderrättelseverksamheten.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Flertalet remissinstanser, däribland *Försvarets radioanstalt*, *Försvarsmakten*, *Säkerhetspolisen*, *Förvaltningsrätten i Stockholm*, *Integritetsskyddsmyndigheten*, *Justitiekanslern* och *Riksarkivet* tillstyrker eller har inga synpunkter på förslaget. *Statens inspektion för försvarsunderrättelseverksamheten* anser att det genom utredningens förslag blir tydligt för allmänheten vilken signalspaning som kan förekomma. *Försvarsunderrättelsedomstolen* föreslår en alternativ författningsteknisk lösning. *Civil Rights Defenders* och *Centrum för rättvisa* menar att man bör avvakta Europadomstolens kommande avgörande i målet Centrum för rättvisa mot Sverige innan utredningens förslag genomförs.

Skälen för regeringens förslag: Internationella samarbeten inom underrättelseområdet är av grundläggande betydelse för svensk underrättelseförmåga. Försvarets radioanstalts deltagande i internationellt samarbete inom myndighetens försvarsunderrättelse- och utvecklingsverksamhet utgör en integrerad och viktig del i myndighetens arbete. Ett fungerande och effektivt internationellt samarbete är en förutsättning för att Försvarets radioanstalt på ett fullgott sätt ska kunna tillgodose det underrättelsebehov som finns hos regeringen och övriga inriktande myndigheter. För att säkerställa att Sverige ska kunna få del av sådan information som landet behöver är det för Försvarets radioanstalt nödvändigt att upprätthålla samarbeten rörande såväl inhämtning, bearbetning, analys, teknik som utbyte av underrättelser. Genom internationella signalspaningssamarbeten möjliggörs svensk tillgång till unik och för svenska underrättelse- och säkerhetsintressen oundgänglig information som annars skulle ligga utanför Försvarets radioanstalts egen kapacitet och räckvidd när det gäller signalspaning. Just inhämtningssamarbeten är av central betydelse för att utöka Försvarets radioanstalts signalspanings geografiska räckvidd. Ett inslag i förtroendefulla underrättelsesamarbeten är att kunna dela information som är värdefull för

samarbetsparten, men som inte alltid är av omedelbar betydelse för det egna landet.

Att under vissa förutsättningar kunna dela information med den utländska myndigheten innebär att Försvarets radioanstalt i olika former skapar incitament för motparten att i sin tur beakta primärt svenska informationsbehov och lämna sådan information tillbaka. Utöver att på så sätt åstadkomma en utökad geografisk räckvidd för Försvarets radioanstalts signalspaning, och motsvarande för en samarbetspart, bidrar förtroendefulla samarbeten påtagligt till möjligheterna att möta den dynamiska och accelererande teknik- och telekommunikationsutveckling som fortlöpande ställer signalspaningen inför nya utmaningar och som inget land ensamt förmår möta. Internationella samarbeten är således av avgörande betydelse för svensk utrikes-, säkerhets- och försvarspolitik och i övrigt vid kartläggning av yttre hot mot landet.

Försvarets radioanstalt får endast inhämta signaler i elektronisk form för de ändamål som anges i lagen om signalspaning i försvarsunderrättelseverksamhet och enbart under förutsättning att Försvarsunderrättelsedomstolen har beslutat att ge tillstånd till inhämtningen (se avsnitt 4.4.1). Flertalet av dessa ändamål är formulerade på ett sätt som ger uttryck för att företeelserna i fråga ska vara riktade mot Sverige eller röra svenska intressen. Även om samarbetande länders underrättelsebehov ofta sammanfaller på ett övergripande nivå kan de enskilda behoven skilja sig åt i fråga om detaljerna. Ett sådant exempel är den internationella terrorismen som utgör ett hot som är påtagligt för många länder, men där ett visst land kan ha ett särskilt intresse för specifika terroristceller som bedöms utgöra ett hot mot det egna landet eller mot det egna landets intressen. Regeringen anser, i likhet med utredningen, att detta förhållande bör komma till tydligt uttryck i regelverket.

Det bör således i lagen om signalspaning i försvarsunderrättelseverksamhet föras in en bestämmelse som innebär att de företeelser för vilka signalspaningsmyndigheten enligt lagen får bedriva signalspaning i försvarsunderrättelseverksamhet i syfte att kartlägga inte behöver vara riktade mot Sverige eller röra svenska intressen. Som utredningen föreslår bör detta gälla enbart om signalspaningen är nödvändig för sådant samarbete i underrättelsefrågor med andra länder och internationella organisationer som signalspaningsmyndigheten deltar i. *Försvarsunderrättelsedomstolen* föreslår en annan författningsteknisk lösning. Regeringen föredrar dock utredningens lagtextförslag.

Med anledning av vad Försvarsunderrättelsedomstolen anför om den proportionalitetsbedömning som domstolen ska göra i sin verksamhet vill regeringen understryka att förslaget inte inverkar på kraven enligt lagen om signalspaning i försvarsunderrättelseverksamhet när det gäller vad en anmälan till domstolen ska innehålla i fråga om t.ex. sökbegrepp eller kategorier av sökbegrepp som är avsedda att användas vid inhämtningen. Förslaget inverkar inte heller på de bestämmelser som rör Statens inspektion för försvarsunderrättelseverksamhetens kontrollansvar.

Civil Rights Defenders och *Centrum för rättvisa* menar att man bör avvakta Europadomstolens kommande avgörande i målet Centrum för rättvisa mot Sverige (35252/08) innan utredningens förslag genomförs. Europadomstolen har den 25 maj 2021 meddelat sitt avgörande i målet och funnit att den svenska lagstiftningen om signalspaning i försvars-

underrättelseverksamhet i huvudsak är förenlig med Europakonventionen. Domstolen framhåller i domen särskilt att lagstiftningen innehåller tydliga regler avseende vilka syften som kan rättfärdiga signalspaning samt hur förfarandet går till. Däremot identifierar domstolen brister i några avseenden. Ett analysarbete kring avgörandet har inletts inom Regeringskansliet.

Regeringen behandlar i avsnitt 10.5 en av Europadomstolens synpunkter på den svenska lagstiftningen. Regeringen har i propositionen Totalförsvaret 2021–2025 aviserat att en särskild utredare bör under perioden 2021–2025 ges i uppdrag att göra en översyn av lagen om signalspaning i försvarsunderrättelseverksamhet. I översynen bör bl.a. frågan om behovet av åtgärder i övrigt med anledning av Europadomstolens avgörande ingå (jfr prop. 2020/21:30 s. 155).

Mot denna bakgrund anser regeringen att det inte finns skäl att avvakta med att genomföra utredningens förslag.

15.2 Regeringen ska inrikta signalspaningen vid internationellt samarbete

Regeringens förslag: Regeringen ska bestämma inriktningen av sådan signalspaning som bedrivs inom ramen för signalspaningsmyndighetens internationella samarbete i försvarsunderrättelseverksamheten.

Utredningens förslag stämmer i sak överens med regeringens.

Remissinstanserna: Flertalet remissinstanser, däribland *Försvarets radioanstalt*, tillstyrker eller invänder inte mot utredningens förslag.

Skälen för regeringens förslag: Inriktning av signalspaning i försvarsunderrättelseverksamhet enligt lagen om signalspaning i försvarsunderrättelseverksamhet får endast anges av regeringen, Regeringskansliet, Försvarsmakten, Säkerhetspolisen och Nationella operativa avdelningen i Polismyndigheten. Regeringen bestämmer ensam inriktningen av Försvarets radioanstalts utvecklingsverksamhet.

Regeringens exklusiva inriktningsrätt omfattar även Försvarets radioanstalts internationella samarbete inom utvecklingsverksamheten. Detta framgår av 4 § andra stycket lagen om signalspaning i försvarsunderrättelseverksamhet.

Internationellt samarbete inom försvarsunderrättelseområdet har tydliga utrikes-, säkerhets- och försvarspolitiska aspekter. Det är också regeringen som enligt lagen om försvarsunderrättelseverksamhet och lagen om signalspaning i försvarsunderrättelseverksamhet ansvarar för att närmare bestämma det samarbete i underrättelse- och signalspaningsfrågor med andra länder och internationella organisationer som Försvarets radioanstalt får etablera och upprätthålla. Regeringen anser därför, i likhet med utredningen och flertalet remissinstanser, att enbart regeringen bör bestämma inriktningen av sådan signalspaning som bedrivs inom ramen för Försvarets radioanstalts internationella samarbete i myndighetens försvarsunderrättelseverksamhet. Lagtexten bör utformas i enlighet med detta.

15.3 Förstöringsskyldigheten preciseras

Regeringens förslag: Signaler som utväxlas autonomt mellan tekniska system och som inte innehåller personuppgifter ska inte behöva förstöras hos Försvarets radioanstalt. Detsamma ska gälla för uppgifter som sänds till eller från utländsk militär personal som befinner sig på svenskt territorium.

Det ska framgå av lagen om signalspaning i försvarsunderrättelseverksamhet att bestämmelserna om förstöringsskyldighet även gäller för upptagningar och uppteckningar som Försvarets radioanstalt har fått från ett annat land eller en internationell organisation inom ramen för ett internationellt samarbete.

Utredningen om behandlingen av personuppgifter vid Försvarsmakten och Försvarets radioanstalts förslag överensstämmer delvis med regeringens. Utredningens förslag omfattar inte uppgifter som sänds till eller från utländsk militär personal som befinner sig på svenskt territorium.

Remissinstanserna: Flertalet remissinstanser tillstyrker eller invänder inte mot utredningens förslag. *Försvarets radioanstalt*, som välkomnar utredningens förslag, föreslår att myndigheten även ska kunna inhämta signaler som sänds från eller till utländsk militär personal som befinner sig på svenskt territorium utan att personalen behöver befinna sig på ett utländskt statsfartyg, statsluftfartyg eller ett militärt fordon. *Datainspektionen* delar utredningens bedömning att signaler som inte innehåller personuppgifter kan undantas från förbudet mot inhämtning som avser signaler mellan en avsändare och mottagare som båda befinner sig i Sverige. Enligt myndigheten bör gränsdragningsproblematiken med olika typer av tekniska signaler och svårigheterna att avgöra om det är sådana rent tekniska signaler som inte innehåller personuppgifter utvecklas vidare i det fortsatta lagstiftningsarbetet. *Statens inspektion för försvarsunderrättelseverksamheten* anser att det bör tydliggöras i vilka andra sammanhang än vid teknisk signalspaning till stöd för produktion av signalreferensbibliotek som det förekommer signaler som utväxlas autonomt i och mellan tekniska system där ingen mänsklig information förekommer och inga integritetsaspekter gör sig gällande.

Utredningen om regleringen av Försvarets radioanstalts internationella samarbetes förslag överensstämmer med regeringens.

Remissinstanserna: Flertalet remissinstanser, däribland *Försvarets radioanstalt*, *Försvarsmakten*, *Säkerhetspolisen*, *Centrum för rättvisa*, *Civil Rights Defenders*, *Polismyndigheten* och *Förvaltningsrätten i Stockholm*, tillstyrker eller invänder inte mot utredningens förslag. *Integritetsskyddsmyndigheten* och *Sveriges advokatsamfund* ser positivt på förslaget ur ett integritetsskyddsperspektiv. Civil Rights Defenders anser att innebörden av orden avsändare och mottagare bör förtydligas.

Skälen för regeringens förslag

Vissa inhämtade uppgifter ska inte behöva förstöras

Enligt lagen om signalspaning i försvarsunderrättelseverksamhet 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 upptecknin gen förstöras så snart det står klart att sådana signaler har inhämtats. Detta gäller dock inte för signaler mellan sändare och mottagare på utländska statsfartyg, statsluftfartyg och militära fordon. Regleringen gäller såväl kommunikationsspaning, dvs. mänsklig kommunikation, som teknisk signalspaning (2 a §). I propositionen Förstärkt integritetsskydd vid signalspaning har regeringen uttalat att signalspaning inte får avse inhemsk trafik (prop. 2008/09:201 s. 40–42). *Civil Rights Defenders* efterfrågar förtydliganden i fråga om orden avsändare och mottagare i lagen. Regeringen anser inte att det finns behov av detta.

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.

Försvarets radioanstalt inhämtar och analyserar radarsignaler inom ramen för den tekniska signalspaningen i syfte att identifiera dem och associera dem till den 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 bestämmelser i förordning har till uppgift att vidmakthålla och utveckla för Försvarsmaktens behov (3 c § förordningen med instruktion för Försvarets radioanstalt). 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. När det gäller signaler mellan sändare och mottagare på utländska statsfartyg, statsluftfartyg och militära fordon som befinner sig i Sverige är inhämtning likaledes möjlig enligt undantagsregeln. I andra fall är det inte lika tydligt huruvida nuvarande reglering ger stöd för att mäta signaler som utgår från svenskt territorium. Vad gäller radarsignaler kan det hävdas att det inte är fråga om signaler mellan avsändare och mottagare i lagens mening och därmed inte heller signaler mellan en avsändare och mottagare som befinner sig i Sverige, eftersom samma radarsignal utgår och återkommer till samma radarutrustning. Ett annat synsätt kan vara att betrakta det objekt som radarsignalen studsar mot som sändare. Det är dock den som sänder ut radarsignalen, inte Försvarets radioanstalt, som kan registrera på vilket objekt som signalen studsar.

De ovan beskrivna signalerna innehåller inte några uppgifter om mänsklig kommunikation och en inhämtning av dem aktualiserar därmed inte frågan om personrelaterad integritet. Som utredningen föreslår bör undantaget från kravet på förstöring därför även omfatta signaler som utväxlas autonomt mellan tekniska system och inte innehåller personuppgifter. Lagtexten bör utformas i enlighet med detta.

Statens inspektion för försvarsunderrättelseverksamheten anser att det bör tydliggöras i vilka andra sammanhang än vid teknisk signalspaning till stöd för produktion av signalreferensbibliotek som det förekommer signaler som utväxlas autonomt i och mellan tekniska system där ingen mänsklig information förekommer och där inga integritetsaspekter gör sig gällande. Ett exempel är sådana tekniska signaler utan mänsklig kommunikation som inhämtas inom ramen för Försvarets radioanstalts utvecklingsverksamhet för att följa förändringar i signalmiljön i omvärlden.

Som *Försvarets radioanstalt* uppmärksammar innebär nuvarande reglering att myndigheten inte får inhämta signaler mellan främmande makts specialförbandssoldater som rör sig till fots i svensk terräng, fälls från luften i svenskt luftrum eller rör sig i svenska vatten. Det skulle kunna vara fråga om förtrupper med sabotage- och underrättelseuppgifter, t.ex. inför att reguljära förband ska rycka fram i sådana fordon som anges i befintligt undantag. Specialförband kan även utgöra verktyg för främmande makt vid kris eller s.k. gråzonssituationer där dolda operationer på svenskt territorium kan vara inslag i försök att påverka utvecklingen i Sverige i den riktning främmande makt önskar. En annan tänkbar situation avser fall då utländsk militär personal kommunicerar med någon som inte befinner sig på ett utländskt statsfartyg, statsluftfartyg eller militärt fordon. Det kan vara fråga om andra representanter för främmande makt, men också deltagare i en motståndsrörelse i Sverige som stöder en främmande makt, allt under förutsättning att det är fråga om utländska förhållanden enligt lagen om försvarsunderrättelseverksamhet.

Regeringen föreslår mot denna bakgrund att Försvarets radioanstalt även ska kunna inhämta signaler som sänds till eller från utländsk militär personal som befinner sig på svenskt territorium, utan att personalen behöver befinna sig på ett utländskt statsfartyg, statsluftfartyg eller ett militärt fordon.

Den reglerade förstöringsskyldigheten gäller även vid internationellt samarbete

Inhämtning i signalspaning i försvarsunderrättelseverksamhet får, som redovisas ovan, 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 (2 a § lagen om signalspaning i försvarsunderrättelseverksamhet). En omedelbar förstöringsskyldighet föreligger också för en upptagning eller uppteckning av uppgifter som har inhämtats enligt lagen och innehållet

1. berör en viss fysisk person och har bedömts sakna betydelse för verksamhet som avses i 1 § lagen om signalspaning i försvarsunderrättelseverksamhet,
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. 5 § tryckfrihetsförordningen eller 2 kap. 5 § 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 sådana inhämtningssyften som gäller för signalspaning i försvarsunderrättelseverksamhet (7 § lagen om signalspaning i försvarsunderrättelseverksamhet).

Inom ramen för det internationella underrättelse- och säkerhetssamarbetet tar Försvarets radioanstalt emot upptagningar och uppteckningar från andra länders underrättelse- och säkerhetstjänster och internationella organisationer. Det kan inte uteslutas att ett annat land eller en internationell organisation i sin signalspaningsverksamhet oavsiktligt har inhämtat upptagningar eller uppteckningar som enligt lagen om signalspaning i försvarsunderrättelseverksamhet måste förstöras om Försvarets radioanstalt hade inhämtat dem i sin egen signalspaningsverksamhet. Försvarets radioanstalt har upplyst utredningen om att myndigheten förstör mottagna upptagningar och uppteckningar om det vid en analys framkommer att det är fråga om en sådan situation.

Som utredningen föreslår bör denna ordning komma till uttryck i lagen om signalspaning i försvarsunderrättelseverksamhet. Det bör således i lagen införas bestämmelser som innebär att förstöringsskyldigheten även gäller för upptagningar eller uppteckningar som signalspaningsmyndigheten har fått från ett annat land eller en internationell organisation inom ramen för ett internationellt samarbete.

I linje med vad bl.a. *Integritetsskyddsmyndigheten* och *Sveriges advokatsamfund* anför bedömer regeringen att förslaget ytterligare bidrar till att stärka skyddet för den personliga integriteten.

16 Följdändringar i andra författningar

Regeringens förslag: I lagen med kompletterande bestämmelser till EU:s dataskyddsförordning införs hänvisningar till lagen om behandling av personuppgifter vid Försvarsmakten och lagen om behandling av personuppgifter vid Försvarets radioanstalt.

I brottsdatalagen införs en hänvisning till lagen om behandling av personuppgifter vid Försvarsmakten.

I lagen om signalspaning i försvarsunderrättelseverksamhet införs en hänvisning till lagen om behandling av personuppgifter vid Försvarets radioanstalt.

Nuvarande hänvisningar i lagarna till lagen om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst och lagen om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet tas bort.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna yttrar sig inte särskilt över utredningens förslag.

Skälen för regeringens förslag: I enlighet med utredningens förslag bör de hänvisningar till FM-PuL och FRA-PuL som finns i 1 kap. 3 § 1 dataskyddslagen ändras så att hänvisningar i stället görs till de nya lagarna.

Den hänvisning till FM-PUL som finns i 1 kap. 4 § brottsdatalagen bör i enlighet med utredningens förslag ändras så att hänvisningen i stället avser den nya lagen om behandling av personuppgifter vid Försvarsmakten.

I enlighet med utredningens förslag bör den hänvisning till FRA-PuL som finns i 12 a § lagen om signalspaning i försvarsunderrättelseverksamhet ändras så att hänvisningen i stället avser den nya lagen om behandling av personuppgifter vid Försvarets radioanstalt.

17 Ikraftträdande- och övergångsbestämmelser

Regeringens förslag: De nya lagarna och övriga lagändringar ska träda i kraft den 1 januari 2022.

Genom de nya lagarna upphävs lagen om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst och lagen om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet.

Äldre föreskrifter ska fortsätta att gälla för överklagande av beslut som har meddelats före de nya lagarnas ikraftträdande.

Punkt 3 i ikraftträdande- och övergångsbestämmelserna till dataskyddslagen upphävs.

Utredningarnas förslag överensstämmer delvis med regeringens. Utredningen om behandlingen av personuppgifter vid Försvarsmakten och Försvarets radioanstalt föreslår ett tidigare ikraftträdande och föreslår inte att punkt 3 i ikraftträdande- och övergångsbestämmelsen till dataskyddslagen ska upphävas. Utredningen föreslår vidare en övergångsbestämmelse om tillsyn och granskning, men inte om överklagande av beslut som har meddelats före de nya lagarnas ikraftträdande.

Remissinstanserna yttrar sig inte särskilt över utredningarnas förslag.

Skälen för regeringens förslag

Ikraftträdande

De nya lagarna och övriga lagändringar bör lämpligen träda i kraft den 1 januari 2022. Eftersom de nya lagarna ersätter lagen om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst och lagen om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet bör de befintliga författningarna upphävas samtidigt som de nya lagarna träder i kraft.

Övergångsbestämmelser till de nya lagarna

I frågor som rör behandling av personuppgifter hos Försvarsmakten och Försvarets radioanstalt bör den nya lagstiftningen tillämpas från det att den träder i kraft. Det innebär exempelvis att framställningar om att få ta del av information, ärenden om rättelse och andra oavslutade ärenden ska hanteras enligt de nya lagarna. Någon övergångsbestämmelse för de båda myndigheternas handläggning behövs därmed inte.

När det gäller tillsynsåtgärder följer det av allmänna principer att beslut om förelägganden, t.ex. i form av förbud, som har meddelats med stöd av personuppgiftslagen och som rör de nya lagarnas tillämpningsområden fortsätter att gälla efter det att övergångsregleringen i denna del har upphävts. Det behövs därför inte någon särskild övergångsbestämmelse om detta.

För andra frågor om tillsyn över behandling av personuppgifter inom de nya lagarnas tillämpningsområden föreslår utredningen att äldre föreskrifter ska fortsätta att gälla för de ärenden som har påbörjats före ikraftträdandet, men inte hunnit avgöras när den nya lagen träder i kraft. I propositionen om en ny dataskyddslag föreslog regeringen inte någon motsvarande övergångsbestämmelse. Regeringen gjorde bedömningen att det saknas skäl för en sådan övergångsbestämmelse eftersom Datainspektionen påpekat att pågående behandling ska bedömas enligt regleringen i dataskyddsförordningen när den börjar tillämpas (se prop. 207/18:105 s. 175–176. Motsvarande bedömning gjordes i förarbetena till brottsdatalagen (prop. 2017/18:232 s. 424) och lagen om Säkerhetspolisens behandling av personuppgifter (prop. 2018/19:163 s. 206–207). Mot denna bakgrund anser regeringen att det inte heller bör införas någon sådan övergångsbestämmelse till de nya lagarna.

Det följer av allmänna rättsgrundsatser att ny lagstiftning ska gälla i fråga om skadestånd med anledning av skadefall som inträffar efter ikraftträdandet, medan äldre lag ska tillämpas på skadefall som har inträffat dessförinnan (Kungl. Maj:ts proposition med förslag till skadeståndslag m.m., prop. 1972:5 s. 593 och prop. 2017/18:105 s. 176). Någon särskild övergångsbestämmelse om detta behövs därför inte.

Enligt FM-PuL, FRA-PuL och personuppgiftslagen får vissa beslut av Försvarsmakten och Försvarets radioanstalt överklagas. Enligt personuppgiftslagen får även tillsynsmyndighetens beslut överklagas. Utredningen föreslår inte någon övergångsbestämmelse i fråga om överklagande av beslut som har meddelats före de nya lagarnas ikraftträdande. Regeringen anser att en sådan bestämmelse bör införas. Det innebär bl.a. att en domstol vid prövningen av ett sådant överklagande ska tillämpa de upphävda lagarna.

Upphävande av en övergångsbestämmelse till dataskyddslagen

Enligt punkt 3 i ikraftträdande- och övergångsbestämmelserna till dataskyddslagen ska den upphävda personuppgiftslagen fortsätta att gälla i sådan verksamhet hos Försvarsmakten och Försvarets radioanstalt som inte omfattas av unionsrätten.

Övergångsbestämmelsen, som ursprungligen även omfattade Totalförsvarets rekryteringsmyndighet, tillkom med anledning av det pågående översynsarbete av de särskilda regleringar som gäller för

Försvarsmaktens, Försvarets radioanstalts respektive Totalförsvarets rekryteringsmyndighets behandling av personuppgifter som bedrevs vid tiden för dataskyddslagens tillkomst. Regeringen uttalade i propositionen Ny dataskyddslag att bestämmelsen är av övergångskaraktär och att den ska upphävas i samband med att den anpassade regleringen om behandling av personuppgifter i dessa myndigheters verksamhet träder i kraft (prop. 2017/18:105 s. 172). Regleringen om Totalförsvarets rekryteringsmyndighet utgick ur övergångsbestämmelsen när den nya totalförsvarsdatalagen trädde i kraft den 1 maj 2020.

När de nya lagarna träder i kraft kan punkt 3 i ikraftträdande- och övergångsbestämmelsen till dataskyddslagen upphävas.

18 Konsekvenser

Regeringens bedömning: Förslagen till nya lagar medför ökad tydlighet för berörda myndigheter, men innebär inte några nya uppgifter.

Förslaget till ändringar i lagen om signalspaning i försvarsunderrättelseverksamhet innebär en mer preciserad reglering av Försvarets radioanstalts internationella samarbete samtidigt som enskildas rättigheter tydliggörs.

Förslagen medför inga ökade kostnader för det allmänna. Förslagen medför inte heller ökade kostnader för enskilda och förväntas inte medföra några konsekvenser av betydelse i övrigt.

Utredningarnas bedömningar överensstämmer i sak med regeringens bedömning.

Remissinstanserna: Remissinstanserna yttrar sig inte särskilt över utredningens bedömning i SOU 2018:63. *Statens inspektion för försvarsunderrättelseverksamheten* bedömer att lagförslaget i SOU 2020:68 kan medföra ytterligare granskningsinsatser, vilket kan leda till behov av utökade medel för myndigheten.

Skälen för regeringens bedömning

Konsekvenser för Försvarsmakten och Försvarets radioanstalt

De föreslagna lagarna medför inga nya uppgifter för Försvarsmakten och Försvarets radioanstalt. Lagarna ansluter också till stora delar till vad som gäller enligt nuvarande regelverk. De föreslagna ändringarna i lagen om signalspaning i försvarsunderrättelseverksamhet innebär inte heller några nya uppgifter för Försvarets radioanstalt.

Ökade möjligheter för direktåtkomst för Försvarsmakten, Försvarets radioanstalt och Säkerhetspolisen i försvarsunderrättelseverksamheten bör kunna öka myndigheternas effektivitet på det området. För Försvarsmaktens del innebär ökade möjligheter till annat elektroniskt informationsutbyte ytterligare effektivisering av verksamheten. Regleringen för vilka andra ändamål än huvudändamålen som behandling av personuppgifter får ske i Försvarets radioanstalts verksamheter innebär

förtydliganden som är till nytta för såväl myndigheten som enskilda. Motsvarande gäller förslaget om en ny ändamålsbestämmelse för internationellt samarbete i försvarsunderrättelsefrågor.

Den nya regleringen kan medföra ett visst behov av utbildning av Försvarsmaktens och Försvarets radioanstalts personal utöver den utbildningsverksamhet som myndigheterna redan nu bedriver. De kostnader som detta kan medföra bör kunna rymmas inom myndigheternas befintliga ekonomiska ramar. Nya interna föreskrifter och styrande dokument som kan komma att krävas med anledning av den nya lagstiftningen får anses ingå i myndigheternas ordinarie verksamhet.

Konsekvenser för andra myndigheter

Integritetsskyddsmyndighetens tillsyn och Statens inspektion för försvarsunderrättelseverksamhetens granskning av Försvarsmaktens och Försvarets radioanstalts behandling av personuppgifter föreslås i huvudsak bedrivas på samma sätt som enligt gällande rätt. Förslagen bedöms därmed inte leda till några merkostnader för dessa myndigheter. Enligt *Statens inspektion för försvarsunderrättelseverksamheten* kan lagförslaget i SOU 2020:68 medföra ytterligare granskningsinsatser, vilket kan leda till behov av utökade medel för myndigheten. Regeringen bedömer att de ändringar som föreslås i lagen om signalspaning i försvarsunderrättelseverksamhet inte är av sådan karaktär att de bör påverka Statens inspektion för försvarsunderrättelseverksamhetens förmåga att kunna utföra sin roll som kontrollmyndighet inom befintliga ekonomiska ramar.

Förslaget om en ny ändamålsbestämmelse i lagen om signalspaning i försvarsunderrättelseverksamheten berör Försvarsunderrättelsedomstolen. Förslaget bedöms inte påverka domstolens verksamhet.

Förslagen till nya lagar för behandling av personuppgifter berör de allmänna förvaltningsdomstolarna. Möjligheten att överklaga beslut av det slag som föreslås finns till stor del redan enligt nuvarande ordning. Förslaget bedöms inte innebära någon måltillströmning av betydelse och bedöms därför inte påverka domstolarnas verksamhet i någon omfattning som ställer krav på ytterligare medel.

Förslagen bedöms inte påverka några andra statliga myndigheter.

Konsekvenser för enskilda

De effektiviseringar som de nya lagarna bedöms medföra vid behandling av personuppgifter inom försvarsunderrättelseverksamheten och den militära säkerhetstjänsten, t.ex. när det gäller möjligheter till direktåtkomst, kan innebära ett visst ytterligare intrång i den enskildes personliga integritet. Integritetsintrånget måste dock vägas mot de starka försvars- och säkerhetsintressen som gör sig gällande och som motiverar behovet av en effektiv verksamhet på de områden som de föreslagna lagarna omfattar. Den omfattande tillsyn och krav på granskning som redan gäller och fortsatt ska gälla för den behandling av personuppgifter som den föreslagna lagstiftningen omfattar är av stor betydelse för tillvaratagandet av den enskildes integritetsskydd. Motsvarande gäller för Statens inspektion för försvarsunderrättelseverksamhetens kontroll av signalspaningen i försvarsunderrättelseverksamhet.

Förslaget om ändringar om förstöringsplikt för vissa uppgifter i lagen om signalspaning i försvarsunderrättelseverksamhet medför att enskildas rättigheter tydliggörs.

Regeringen bedömer sammantaget att konsekvenserna för den enskildes integritet får anses vara acceptabla.

Förslagen medför inte några ekonomiska konsekvenser för enskilda.

Övriga konsekvenser

Förslagen bedöms inte påverka

- den kommunala självstyrelsen,
- brottsligheten och det brottsförebyggande arbetet,
- sysselsättning och offentlig service i olika delar av landet,
- jämställdheten mellan kvinnor och män, eller
- möjligheten att nå de integrationspolitiska målen.

Förslagen bedöms inte heller i övrigt medföra några konsekvenser av betydelse.

19 Författningskommentar

19.1 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.

I paragrafen anges syftet med lagen. Övervägandena finns i avsnitt 6.3.

Enligt paragrafen är syftet med lagen 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. Lagen har alltså två syften och gäller för enbart fysiska personer. Det innebär att juridiska personer inte omfattas av lagen.

Lagens tillämpningsområde

2 § Denna lag gäller vid Försvarsmaktens behandling av personuppgifter i verksamhet som rör Sveriges försvar och säkerhet samt internationellt försvars- och säkerhetssamarbete.

I paragrafen anges lagens tillämpningsområde. Övervägandena finns i avsnitt 6.4.1. Paragrafen utformas efter synpunkter från *Lagrådet*.

I paragrafen anges att lagen gäller vid Försvarsmaktens behandling av personuppgifter i verksamhet som rör Sveriges försvar och säkerhet samt internationellt försvars- och säkerhetssamarbete, dvs. inom verksamhet

som ligger utanför unionsrätten. Uttrycken personuppgift och behandling av personuppgifter definieras i 5 §.

Uttrycket Sveriges försvar och säkerhet omfattar Försvarsmaktens huvuduppgift att försvara Sverige mot ett väpnat angrepp. Även Försvarsmaktens verksamhet som syftar till att främja Sveriges säkerhet, inbegripet Försvarsmaktens egen säkerhet omfattas. Vidare omfattas Försvarsmaktens uppgift att hävda Sveriges territoriella integritet samt förmåga att värna Sveriges suveräna rättigheter och svenska intressen samt att förebygga och hantera konflikter och krig såväl nationellt som internationellt. Försvarsmakten ska kunna utföra sina uppgifter självständigt eller i samverkan med andra myndigheter, stater och organisationer.

Den behandling av personuppgifter som sker inom ramen för dessa verksamheter omfattas av bestämmelsen. Även behandlingen av personuppgifter i Försvarsmaktens interna och administrativa verksamhet som rör myndighetens personal omfattas av lagen. Lagen gäller därmed också för den personuppgiftsbehandling som sker inom ramen för Försvarsmaktens krigsorganisation.

Uttrycket internationellt försvars- och säkerhetssamarbete omfattar det internationella samarbete som Försvarsmakten bedriver med stöd av föreskrifter i förordning eller regeringens beslut i enskilda fall. Lagen omfattar inte Försvarsmaktens behandling av personuppgifter som sker när myndigheten lämnar stöd till civila aktörer i situationer som inte kan knytas till Sveriges försvar eller säkerhet. I sådana fall är EU:s dataskyddsförordning och dataskyddslagen (2018:218) tillämpliga för myndighetens behandling av personuppgifter.

I 2 kap. anges närmare de ändamål för vilka Försvarsmakten får behandla personuppgifter.

3 § Lagen gäller vid sådan behandling av personuppgifter som är helt eller delvis automatiserad. Den gäller också personuppgifter som ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

Paragrafen preciserar lagens tillämpningsområde. Övervägandena finns i avsnitt 6.4.1.

Av paragrafen framgår att lagen gäller vid sådan behandling av personuppgifter som är helt eller delvis automatiserad och också personuppgifter som ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

När det gäller automatiserad behandling krävs det inte att personuppgifterna som behandlas finns i något som kan karaktäriseras som ett register eller att de annars är ordnade på visst sätt. Manuell behandling i t.ex. register omfattas av bestämmelsen om personuppgifterna är tillgängliga för sökning eller sammanställning enligt mer än ett kriterium. Uteslutande manuell behandling av personuppgifter som inte ingår i någon samling och inte heller är avsedda att ingå i en sådan, exempelvis handskrivna minnesanteckningar, ligger däremot utanför tillämpningsområdet.

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

I paragrafen regleras förhållandet till EU:s dataskyddsförordning och lagen med kompletterande bestämmelser till EU:s dataskyddsförordning. Övervägandena finns i avsnitt 6.2.

Av paragrafen framgår att 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) och lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning inte gäller vid behandling av personuppgifter enligt lagen.

Ord och uttryck i lagen

5 § I denna lag används följande ord och uttryck.

Ord och uttryck	*Betydelse*
Behandling av personuppgifter	En åtgärd eller en 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 identifiering av personen i fråga.
Dataskyddsombud	En fysisk person som utses av den personuppgiftsansvarige för att självständigt kontrollera att personuppgifter behandlas författningsenligt och på ett korrekt sätt.
Genetiska uppgifter	Personuppgifter som rör en persons nedärvda eller förvärvade genetiska kännetecken och som framför allt

	härrör från analys av ett spår av eller ett biologiskt prov från personen i fråga.
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 behandlar personuppgifter för den personuppgiftsansvariges räkning.
Registrerad	Den fysiska person som personuppgiften gäller.
Tredje part	Någon annan än – den registrerade, – den 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.

I paragrafen definieras vissa ord och uttryck som används i lagen.

Behandling av personuppgifter

Uttrycket behandling av personuppgifter omfattar alla åtgärder som vidtas med sådana uppgifter. Uttrycket behandlas i avsnitt 6.5.

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

Biometri är en samlingsbenämning för sådan automatiserad teknik som syftar till att identifiera en person eller avgöra om en påstådd identitet är riktig. Uttrycket behandlas i avsnitt 6.5.

Den automatiserade tekniken 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 för närvarande 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 författningskommentaren 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 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. Fotografier kan omfattas av regleringen om känsliga personuppgifter även på andra grunder, se författningskommentaren till 2 kap. 15 §.

Dataskyddsombud

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. Ordet behandlas i avsnitt 11.4.

Ett dataskyddsombud ska vara anställt hos den personuppgiftsansvarige. Kravet på självständighet innebär att dataskyddsombud ska kunna utföra sina arbetsuppgifter på ett oberoende sätt. Ombuden förutsätts framför allt ha goda kunskaper om regelverket om personuppgiftsbehandling. Ombuden bör också ha sådan ställning i organisationen att det säkerställs att deras synpunkter och råd beaktas.

Genetiska uppgifter

Med uttrycket genetiska uppgifter avses personuppgifter som rör en persons nedärvda eller förvärvade genetiska kännetecken och som framför allt härrör från analys av ett spår av eller ett biologiskt prov från personen i fråga. Det är alltså fråga om all information som rör en persons nedärvda eller förvärvade genetiska kännetecken och som kan tas fram ur ett spår från människokroppen. Uttrycket behandlas i avsnitt 6.5.

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. Den dna-profil som behandlas i ett dna-register utgör däremot inte en genetisk uppgift, eftersom inga nedärvda eller förvärvade genetiska kännetecken kan utläsas ur den. En dna-profil är i stället en biometrisk uppgift, eftersom den tas fram genom en särskild teknisk behandling av en persons arvsmassa för att möjliggöra eller bekräfta identifiering av personen i fråga.

Mottagare

Mottagare definieras som den till vilken personuppgifter lämnas ut, med undantag av en myndighet som med stöd av författning utövar tillsyn, kontroll eller revision. Ordet behandlas i avsnitt 6.5.

Undantaget omfattar bl.a. myndigheter som tar del av personuppgifter i sin tillsyn och kontroll av viss verksamhet, t.ex. Integritetsskyddsmyndigheten och Statens inspektion för försvarsunderrättelseverksamheten. Även andra myndigheter som utövar tillsyn, t.ex. Riksdagens ombudsmän (JO) och Justitiekanslern, omfattas av undantaget.

Personuppgift

Med personuppgift avses varje upplysning om en identifierad eller identifierbar fysisk person som är i livet. Ordet behandlas i avsnitt 6.5.

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.

Uppgifter om juridiska personer omfattas inte av definitionen.

Personuppgiftsansvarig

Personuppgiftsansvarig är enligt definitionen den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter. Ordet behandlas i avsnitt 11.1.

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

Ett personuppgiftsbiträde är en fysisk eller juridisk person som behandlar personuppgifter för den personuppgiftsansvariges räkning. Ordet behandlas i avsnitt 11.5.1.

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.

Registrerad

Med registrerad avses den fysiska person som en personuppgift rör. Ordet behandlas i avsnitt 6.5.

Av definitionen av personuppgift framgår bl.a. att personen ska vara i livet.

Tredje part

Tredje part är någon annan än den registrerade, personuppgiftsansvarige, dataskyddsombudet, personuppgiftsbiträdet, och sådana personer som under den personuppgiftsansvarige eller personuppgiftsbiträdets direkta ansvar har rätt att behandla personuppgifter. Uttrycket behandlas i avsnitt 6.5.

Uppgiftssamling

Uppgiftssamling är en samling med uppgifter som med hjälp av automatiserad behandling är gemensamt tillgängliga. Ordet behandlas i avsnitt 6.5.

Avgörande för när automatiserat behandlade uppgifter ska anses ingå i en uppgiftssamling är att uppgifterna är gemensamt tillgängliga i Försvarsmaktens verksamhet enligt vad som framgår av lagen och föreskrifter som har meddelats i anslutning till lagen.

Personuppgiftsansvar

6 § Försvarsmakten är personuppgiftsansvarig för all behandling av personuppgifter som myndigheten utför, som utförs under myndighetens ledning eller på dess vägnar.

Paragrafen reglerar personuppgiftsansvar. Övervägandena finns i avsnitt 11.1. Paragrafen utformas enligt *Lagrådets* förslag.

I *paragrafen* anges att Försvarsmakten är personuppgiftsansvarig för all behandling av personuppgifter som myndigheten utför, som utförs under myndighetens ledning eller på dess vägnar. Den närmare innebörden av personuppgiftsansvaret framgår av övriga bestämmelser i lagen och föreskrifter som har meddelats i anslutning till lagen.

Personuppgiftsansvaret omfattar alltså all behandling av personuppgifter som utförs vid myndigheten. Det gäller både behandling som utförs genom en aktiv handling, t.ex. insamling eller sökning, och passiv behandling, t.ex. lagring. Ansvaret omfattar däremot inte sådan

behandling som myndigheten utför i egenskap av personuppgiftsbiträde. Genom att ansvaret knyts till behandling som utförs under Försvarsmaktens ledning tydliggörs att det inte är myndigheten som utför personuppgiftsbehandlingen utan de anställda.

Försvarsmakten är också ansvarig för den behandling av personuppgifter som utförs på myndighetens 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. Personuppgiftsansvaret sträcker sig då utanför Försvarsmaktens egen verksamhet. Personuppgiftsbiträdets behandling ska styras av skriftliga avtal eller andra skriftliga överenskommelser och får endast utföras enligt instruktioner från Försvarsmakten, se författningskommentarerna till 4 kap. 7 och 9 §§.

Två eller flera personuppgiftsansvariga kan behandla samma personuppgifter samtidigt för olika ändamål, t.ex. om de har direktåtkomst till personuppgifter i samma system. Varje personuppgiftsansvarig är då ansvarig för den behandling som utförs under dennes ledning eller på dennes vägnar.

2 kap. Behandling av personuppgifter

Grundläggande krav på behandlingen

Krav på ändamål

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

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

I paragrafen regleras grundläggande krav på behandlingen av personuppgifter i fråga om krav på ändamål. Övervägandena finns i avsnitt 7.1.

Enligt *första stycket* får personuppgifter bara behandlas för särskilda, uttryckligt angivna och berättigade ändamål. Det ställs alltså 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, eller ett särskilt beslut av regeringen. Detta innebär att ändamålen med en behandling av personuppgifter måste bestämmas redan när uppgifterna samlas in.

Av *andra stycket* framgår att personuppgifter inte får behandlas för något ändamål som är oförenligt med det ändamål som de ursprungligen behandlades för. Bestämmelsen ger uttryck för den generella s.k. finalitetsprincipen, dvs. att fortsatt behandling inte får ske för något ändamål som är oförenligt med det ändamål för vilket personuppgifterna ursprungligen behandlades. Vad som kan utgöra oförenliga ändamål måste avgöras i det enskilda fallet. Det innebär att den personuppgiftsansvarige under hela behandlingstiden måste hålla reda på för vilka ändamål varje personuppgift ursprungligen har behandlats för.

2 § 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, kollektivavtal eller annat avtal, eller ett särskilt beslut där regeringen har gett myndigheten i uppdrag att utföra uppgiften.

För Försvarsmaktens behandling av personuppgifter i myndighetens försvarsunderrättelseverksamhet och militära säkerhetstjänst gäller i stället 3–8 §§.

Paragrafen anger vissa ändamål för Försvarsmaktens personuppgiftsbehandling. Övervägandena finns i avsnitt 7.2.1.

Personuppgifter får enligt *första stycket* behandlas av Försvarsmakten om det är nödvändigt för att planera, förbereda och genomföra viss verksamhet.

Enligt *första stycket 1* får personuppgifter behandlas om det är nödvändigt för att planera, förbereda och genomföra verksamhet som rör Sveriges försvar och säkerhet. Bestämmelsen omfattar bl.a. all den verksamhet som krävs för att utveckla och upprätthålla Försvarsmaktens grundläggande uppgift att kunna försvara Sverige mot ett väpnat angrepp.

Bestämmelsen omfattar även myndighetens personaladministrativa verksamhet, som bl.a. utgör en väsentlig del i Försvarsmaktens krigsorganisation. För Försvarsmaktens diarieföring, arkivering, handläggning av ett ärende eller för att utföra en liknande uppgift som myndigheten har finns en ändamålsbestämmelse i 9 §.

Lagen omfattar inte Försvarsmaktens behandling av personuppgifter som sker när myndigheten lämnar stöd till civila aktörer i situationer som inte kan knytas till Sveriges försvar eller säkerhet. I sådana fall är EU:s dataskyddsförordning och dataskyddslagen (2018:218) tillämpliga för myndighetens behandling av personuppgifter (jfr författningskommentaren till 1 kap. 2 §).

Enligt *första stycket 2* får personuppgifter även behandlas om det är nödvändigt för att planera, förbereda och genomföra verksamhet som rör internationellt försvars- och säkerhetssamarbete. Samarbetet kan vara bilateralt eller multilateralt och myndighetens deltagande i sådant samarbete sker med stöd av föreskrifter i förordning eller regeringens beslut i enskilda fall.

Enligt *andra stycket* ska Försvarsmaktens uppgifter att bedriva verksamhet enligt första stycket framgå av lag, förordning, kollektivavtal eller annat avtal, eller ett särskilt beslut där regeringen har gett myndigheten i uppdrag att ansvara för uppgiften. Förfogandelagen (1978:262) och förordningen (2007:1266) med instruktion för Försvarsmakten är exempel på sådana författningar. Tänkbara exempel på annat avtal än kollektivavtal kan vara avtal som Försvarsmakten ingår med en leverantör vid upphandling, med en markägare vid upplåtelse av mark i samband med Försvarsmaktens övningar eller med en fodervärd för en av Försvarsmaktens tjänstehundar.

I *tredje stycket* tydliggörs att ändamålen för behandling av personuppgifter inom Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst finns i 3–8 §§.

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

Paragrafen anger ändamål för vilka personuppgifter får behandlas i Försvarsmaktens försvarsunderrättelseverksamhet. Övervägandena finns i avsnitt 7.2.2.

I paragrafen anges att personuppgifter får behandlas i Försvarsmaktens försvarsunderrättelseverksamhet. En förutsättning för sådan behandling är att det är nödvändigt att bedriva den verksamhet som anges i 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.

I försvarsunderrättelseverksamheten behandlas personuppgifter som avser t.ex. uppgifter om utländsk militär personal, politiker eller andra viktiga befattningshavare. Denna typ av uppgifter är nödvändiga att behandla för att informationsunderlaget för svensk utrikes-, försvars- och säkerhetspolitik ska bli komplett.

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.

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

Första stycket gäller endast om inte något annat följer av denna lag eller en förordning som regeringen har meddelat i anslutning till lagen.

Paragrafen kompletterar 3 § när det är tillåtet att behandla personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet. Övervägandena finns i avsnitt 7.2.2.

I *första stycket* anges 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. Härigenom möjliggörs en fortsatt behandling av personuppgifter som finns inom Försvarsmaktens försvarsunderrättelseverksamhet, under förutsättning att en sådan behandling är nödvändig för att fullgöra den verksamheten. Det möjliggör i sin tur en behandling som inte alltid direkt kan hänföras till regeringens vid varje tidpunkt gällande inriktning av försvarsunderrättelseverksamheten. Det är av grundläggande betydelse att Försvarsmakten kan behandla äldre information, inbegripet person-

uppgifter, för att kunna förstå och bedöma den underrättelsemässiga relevansen av sådant som sker vid den aktuella tidpunkten.

Första stycket gäller endast om inte något annat följer av lagen eller en förordning som regeringen har meddelat i anslutning till lagen. Detta framgår av *andra stycket*.

Militär säkerhetstjänst

5 § 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 anger de ändamål för vilka personuppgifter får behandlas i den militära säkerhetstjänsten. Övervägandena finns i avsnitt 7.2.3.

Ändamålet med behandlingen av personuppgifter inom den militära säkerhetstjänsten är att myndigheten ska kunna fullgöra de uppgifter som följer av bl.a. säkerhetsskyddslagen (2018:585), säkerhetsskyddsförordningen (2018:658) 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 personuppgifter behandlas för att klarlägga verksamhet som innefattar hot mot rikets säkerhet. Därvid får, under de närmare förutsättningar som anges i 6 §, 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.

Av *punkten 2* framgår att personuppgifter får behandlas om det är nödvändigt för att vidta åtgärder som hindrar eller försvårar säkerhetshotande verksamhet. Inom säkerhetsskyddstjänsten 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 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 8 § finns en särskild bestämmelse om personuppgiftsbehandling i signalkontrollverksamheten.

6 § Personuppgifter får behandlas för de ändamål som anges i 5 § endast om

1. personuppgifterna 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 enligt motsvarande äldre föreskrifter,
2. personuppgifterna är nödvändiga för att kartlägga underrättelseverksamhet som riktas mot Försvarsmakten och dess säkerhetsintressen,
3. personuppgifterna är nödvändiga för att kartlägga annan säkerhetshotande verksamhet än som avses i 1 och som innefattar brott eller åsidosättande av skyldigheter i anställning hos Försvarsmakten, om det finns särskilda skäl till att uppgiften ska behandlas,
4. personuppgifterna är nödvändiga för att bedöma om en person som har lämnat uppgifter om säkerhetshotande verksamhet är trovärdig, eller
5. personuppgifterna är nödvändiga för att genomföra säkerhetsprövning enligt säkerhetsskyddslagen (2018:585) eller för att utföra en uppgift som rör säkerhetsskydd.

I paragrafen preciseras de ändamål för vilka personuppgifter får behandlas inom den militära säkerhetstjänsten. Övervägandena finns i avsnitt 7.2.3. Paragrafen utformas enligt *Lagrådets* förslag.

Enligt *punkten 1* får personuppgifter behandlas om de 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 enligt motsvarande brottslighet enligt äldre föreskrifter.

Punkten 2 anger att personuppgifter får behandlas om de är nödvändiga för att kartlägga underrättelseverksamhet som riktas mot Försvarsmakten och dess säkerhetsintressen.

Enligt *punkten 3* får personuppgifterna behandlas om de är nödvändiga för att kartlägga annan säkerhetshotande verksamhet än som avses i punkten 1 och som innefattar brott eller åsidosättande av skyldigheter i anställning hos Försvarsmakten, och det finns särskilda skäl till att uppgiften ska behandlas.

Behandling av personuppgifter får enligt *punkten 4* även ske om personuppgifterna är nödvändiga för att bedöma om en person som har lämnat uppgifter om säkerhetshotande verksamhet är trovärdig.

Enligt *punkten 5* får personuppgifter behandlas om de är nödvändiga för att genomföra säkerhetsprövning enligt säkerhetsskyddslagen (2018:585) eller för att utföra en uppgift som rör säkerhetsskydd. Exempel på uppgifter som rör säkerhetsskydd är Försvarsmaktens tillträdeskontroll vid objekt, lokaler och områden där myndigheten bedriver verksamhet som kräver säkerhetsskydd, men även behörighetshantering inom signalskyddstjänsten, utbildning i säkerhetsskydd och kontroll av säkerhetsloggar omfattas.

7 § Personuppgifter som behandlas enligt 6 § ska förses med upplysning om på vilken av de angivna grunderna uppgiften behandlas.

Om behandlingen av en personuppgift motiveras av något annat än ett antagande om att en person 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 en 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 ett sådant antagande inte finns.

Personuppgifter som behandlas enligt 6 § 1, 2 eller 3 ska i förekommande fall förses med en upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak.

Paragrafen anger närmare villkor som gäller vid personuppgiftsbehandling enligt 6 §. Övervägandena finns i avsnitt 7.2.3.

Enligt *första stycket* ska personuppgifter förses med upplysning om på vilken av de i 6 § angivna grunderna uppgiften behandlas.

Uppgifter om brottsmisstanke är särskilt känsliga från integritetssynpunkt. Det ställs därför i *andra stycket* krav på att detta ska anges särskilt i de fall behandlingen av en personuppgift inte motiveras av antagande om att en person utövar brottslig verksamhet, 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.

Enligt *tredje stycket* ska personuppgifter som avses i 6 § 1, 2 eller 3 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 riktig uppgiften är, t.ex. om det är en obekräftad gissning eller ett belagt faktum.

8 § Trots 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 på 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 6 § 1, 2 eller 3 tillämpas.

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

Paragrafen reglerar ytterligare stöd för Försvarsmakten att behandla personuppgifter inom totalförsvarets telekommunikations- och informationssystem. Övervägandena finns i avsnitt 7.2.4.

I *första stycket* anges 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 på 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 krävs 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 föreligger ett sådant förhållande som avses i 6 § 1, 2 eller 3.

Enligt *andra stycket* ska Försvarsmakten föra en förteckning över de behandlingar som särskilt syftar till att identifiera en person och de uppgifter som utgjort anledningen till behandlingen. Detta möjliggör kontroll av att sådana behandlingar – vilka får anses känsliga från integritetssynpunkt – görs endast i de fall som det är befogat.

Övriga ändamål

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

Paragrafen innehåller förutsättningarna för behandling av personuppgifter i Försvarsmaktens ärendehantering. Övervägandena finns i avsnitt 7.2.5.

Av paragrafen följer att Försvarsmakten får behandla personuppgifter om det är nödvändigt för diarieföring, arkivering, handläggning av ett ärende eller för att utföra annan liknande uppgift som myndigheten har. Bestämmelsen avser ärenden som inleds såväl på Försvarsmaktens eget initiativ som efter framställning av annan. Det kan t.ex. vara fråga om en annan stats ansökan om att få tillträde till svenskt territorium och ärenden om kvalificerade skyddsidentiteter, liksom ärenden i Försvarsmaktens tillsyns- och inspektionsverksamhet eller om utvärdering av den egna verksamheten genom tidredovisning, lönesättning och sjuktal.

Bestämmelsen innebär ett särskilt stöd för Försvarsmakten att behandla personuppgifter om det är nödvändigt för myndighetens diarieföring, arkivering, ärendehandläggning eller för att utföra annan liknande uppgift som myndigheten har (jfr 2 §, som ger stöd för Försvarsmakten att bl.a. behandla personuppgifter inom myndighetens personaladministrativa verksamhet). Det är Försvarsmakten som avgör vilken ändamålsbestämmelse som myndigheten lägger till grund för en viss behandling av personuppgifter.

10 § Försvarsmakten får behandla personuppgifter som utgör allmänt tillgänglig information om det är nödvändigt för den verksamhet som anges i 2, 3 och 5 §§.

Paragrafen ger stöd för behandling av personuppgifter som utgör allmänt tillgänglig information. Övervägandena finns i avsnitt 7.4.

Försvarsmakten får behandla personuppgifter som utgör allmänt tillgänglig information om det är nödvändigt för den verksamhet som anges i 2, 3 och 5 §§. Bestämmelsen gör det möjligt att behandla personuppgifter när det gäller myndighetens verksamhet som avser Sveriges försvar och säkerhet eller internationellt försvars- och säkerhetssamarbete, liksom när det gäller verksamhet inom den militära säkerhetstjänsten.

Även för att kunna bedriva en effektiv försvarsunderrättelseverksamhet behöver Försvarsmakten, utöver den information som myndigheten inhämtar genom särskilda metoder, ha god tillgång till allmänt tillgänglig information. Därigenom kan den på särskilt sätt inhämtade informationen sättas in i sitt rätta sammanhang på ett bättre sätt. Av intresse här är framför allt information som utgörs av personuppgifter som kan påträffas vid sökning på internet eller vid sökningar i öppna databaser.

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

I paragrafen anges att Försvarsmakten får behandla personuppgifter för vetenskapliga, statistiska eller historiska ändamål inom lagens tillämpningsområde. Övervägandena finns i avsnitt 7.5.

Genom bestämmelsen ges Försvarsmakten möjlighet att behandla personuppgifter för vetenskapliga, statistiska eller historiska ändamål.

12 § Försvarsmakten får behandla personuppgifter om lagöverträdelser om det är nödvändigt för myndighetens verksamhet.

Paragrafen innehåller ett preciserat ändamål för behandling av personuppgifter om lagöverträdelser. Övervägandena finns i avsnitt 7.6.

Bestämmelsen ger Försvarsmakten möjlighet att behandla personuppgifter om lagöverträdelser om det är nödvändigt för myndighetens verksamhet. Ett sådant behov kan t.ex. uppkomma inom ramen för Försvarsmaktens militära säkerhetstjänst.

Författningsenlig och korrekt behandling

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

Paragrafen reglerar krav på en författningsenlig och korrekt behandling av personuppgifter. Övervägandena finns i avsnitt 8.1.1.

Enligt paragrafen ska personuppgifter behandlas författningsenligt och på ett korrekt sätt.

Att behandlingen ska ske författningsenligt innebär att den ska ske i enlighet med lag eller annan författning. Författningarna är även av betydelse för att en behandling ska anses ske på ett korrekt sätt. Vad som är ett korrekt sätt för behandling styrs inte enbart av författning. Tillsynsmyndighetens beslut om allmänna råd och uttalanden i fråga om personuppgiftsbehandling har också betydelse, liksom Försvarsmaktens interna regler.

Otillåten behandling av personuppgifter kan i vissa fall vara straffbar enligt bestämmelser i brottsbalken, bl.a. bestämmelsen i 4 kap. 9 c § brottsbalken om dataintrång. Tänkbara exempel på dataintrång kan vara externa angrepp eller att någon som har tillgång till ett it-system överskrider sina befogenheter.

Personuppgifternas kvalitet

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

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 reglerar personuppgifternas kvalitet. Övervägandena finns i avsnitt 8.1.2.

Enligt *första stycket* ska de behandlade uppgifterna vara riktiga och, om det är nödvändigt, uppdaterade. Personuppgifterna ska också vara adekvata och relevanta i förhållande till ändamålet med behandlingen.

En personuppgift är riktig om den stämmer överens med de verkliga förhållandena. För att bestämma vilka de verkliga förhållandena är får man söka ledning i ändamålen med behandlingen. Det är ändamålen i det enskilda fallet som avses. Inom lagens tillämpningsområde måste frågan om en personuppgift är riktig inte bara vägas mot ändamålen med behandlingen utan även ses mot bakgrund av vad uppgiften rör, när den lämnas och vem som lämnar den. För att kunna avgöra om personuppgifterna är riktiga är det också av stor betydelse att veta om de grundar sig på fakta eller på personliga bedömningar. Kravet på att personuppgifter ska vara riktiga innebär inte något hinder mot att samla in exempelvis osäkra underrättelseuppgifter, under förutsättning att personuppgifterna är relevanta för arbetet och att det framgår att det är osäkert om uppgiften är riktig.

De personuppgifter som behandlas behöver vara uppdaterade bara om det är nödvändigt. Frågan om det är nödvändigt att de är uppdaterade får avgöras med hänsyn till ändamålen med behandlingen. Exempelvis kan uppgifter om telefonnummer eller andra kontaktuppgifter ändras under handläggningen av ett ärende och därmed behöva uppdateras.

Att personuppgifterna ska vara adekvata och relevanta innebär att ovidkommande uppgifter inte får behandlas. En prövning av om en personuppgift är nödvändig för behandlingen ska göras kontinuerligt av Försvarsmakten, 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.

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. Uppgifter om utseende är inte i sig att betrakta som känsliga personuppgifter.

Utformningen av stycket innebär att myndigheten alltid är oförhindrad att, om 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 person-

uppgifter 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 personuppgifter behandlas får de dock kompletteras med sådana uppgifter som avses i första stycket, om det är absolut nödvändigt med hänsyn till ändamålen med behandlingen.

Paragrafen, som utformas enligt *Lagrådets* förslag, reglerar känsliga personuppgifter. Övervägandena finns i avsnitt 8.2.

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 typiskt sett 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 sett inte ger upplysning om etniskt ursprung (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.

Andra stycket innehåller ett undantag från huvudregeln att känsliga personuppgifter inte får behandlas. Personuppgifter som behandlas på annan grund får kompletteras med känsliga personuppgifter, om det är absolut nödvändigt med hänsyn till ändamålen med behandlingen. Det innebär att personuppgifter som samlas in i ett visst fall får kompletteras med uppgifter om exempelvis religiös övertygelse eller etniskt ursprung om det är av stor betydelse med hänsyn till ändamålen 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.

Inom den personaladministrativa verksamheten kan t.ex. uppgifter om en enskilds hälsa behöva behandlas inom ramen för ett ärende om sjukfrånvaro eller uppgift om medlemskap i fackförening behöva behandlas inom ramen för ett arbetsrättsligt ärende. I sådana fall är kravet på att behandlingen är absolut nödvändig uppfyllt.

I 16 och 17 §§ finns ytterligare bestämmelser om behandling av känsliga personuppgifter.

Känsliga personuppgifter kan också förekomma i Försvarsmaktens verksamhet på grund av att någon har lämnat en sådan uppgift till myndigheten. 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 enligt andra stycket.

16 § Biometriska uppgifter får behandlas om det är absolut nödvändigt med hänsyn till ändamålen med behandlingen.

Genetiska uppgifter får inte behandlas.

Paragrafen, som utformas enligt *Lagrådets* förslag, reglerar i vilken utsträckning biometriska uppgifter får behandlas. Övervägandena finns i avsnitt 8.2.

Enligt *första stycket* får biometriska uppgifter behandlas om det är absolut nödvändigt med hänsyn till ändamålen med behandlingen Stycket möjliggör användning av särskild teknisk behandling för att bekräfta 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 varje enskilt fall.

I *andra stycket* anges att genetiska uppgifter inte får behandlas. Stycket innebär ett förbud för Försvarsmakten att behandla sådana uppgifter.

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 med hänsyn till ändamålen med behandlingen. Detsamma gäller biometriska uppgifter.

Paragrafen, som utformas enligt *Lagrådets* förslag, reglerar i vilken utsträckning känsliga personuppgifter får användas som sökbegrepp. Övervägandena finns i avsnitt 8.2.

Paragrafen gäller generellt, dvs. för såväl personuppgifter som har gjorts gemensamt tillgängliga som personuppgifter som inte har det.

Paragrafen 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, eller filosofisk övertygelse eller uppgifter som rör hälsa, sexualliv eller sexuell läggning, om sökningen är absolut nödvändig med hänsyn till något av de ändamål för vilket Försvarsmakten behandlar personuppgifter.

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 och samordningsnummer

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

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

Paragrafen reglerar i vilken omfattning personnummer eller samordningsnummer får behandlas vid Försvarsmakten. Övervägandena finns i avsnitt 8.3.

Enligt paragrafen får uppgifter om personnummer eller samordningsnummer bara behandlas när det är klart motiverat med hänsyn till ändamålen med behandlingen (*punkten 1*), vikten av en sådan identifiering (*punkten 2*), eller något annat beaktansvärt skäl (*punkten 3*).

Vad som avses med personnummer och samordningsnummer framgår av folkbokföringslagen (1991:1487). Bestämmelsen innebär att en intresseavvägning mellan behovet av behandlingen och de integritetsrisker som den innebär ska göras. Om behandlingen av personnummer eller samordningsnummer inte är klart motiverad med hänsyn till dess ändamål, till vikten av en säker identifiering eller något annat beaktansvärt skäl får den inte utföras.

Om den registrerade har lämnat sitt samtycke eller offentliggjort personuppgifterna

19 § Trots 15, 16 och 18 §§ får andra personuppgifter än genetiska uppgifter behandlas, om den registrerade har lämnat sitt uttryckliga samtycke eller på ett tydligt sätt har offentliggjort uppgifterna.

Paragrafen reglerar behandling av vissa personuppgifter om den registrerade har lämnat sitt samtycke eller offentliggjort uppgifterna. Övervägandena finns i avsnitt 8.4.

Paragrafen ger Försvarsmakten möjlighet att, med undantag av genetiska uppgifter, behandla känsliga personuppgifter samt personnummer och samordningsnummer, om den registrerade har lämnat sitt uttryckliga samtycke eller på ett tydligt sätt har offentliggjort uppgifterna. Samtyckessituationer kan exempelvis förekomma i Försvarsmaktens militära säkerhetstjänst vid säkerhetsprövningar. Ett tänkbart exempel på offentliggörande kan vara att den registrerade har gjort personuppgifterna tillgängliga på internet.

Behandling av personuppgifter i vissa fall

20 § Hantering av information som innebär behandling av personuppgifter ska inte anses oförenlig med bestämmelserna i 1–3, 5, 6, 8, 10, 12–16 och 18 §§ i det skede av behandlingen då det inte har kunnat fastställas vilka personuppgifter som informationen innehåller.

Paragrafen reglerar behandling av personuppgifter i vissa fall. Övervägandena finns i avsnitt 8.5.

Försvarsmakten kan få information som t.ex. är krypterad och formulerad på ett främmande språk. Innan dess att informationen har bearbetats finns inte förutsättningar för att bedöma om den innehåller personuppgifter. Den initiala behandling som krävs för att detta ska kunna klarläggas måste kunna äga rum utan hinder av bestämmelserna om ändamål, lagöverträdelser, författningsenlig och korrekt behandling, personuppgifternas kvalitet, känsliga personuppgifter samt personnummer och samordningsnummer. Genom bestämmelsen tydliggörs att hantering av information som innebär behandling av personuppgifter inte ska anses oförenlig med bestämmelserna i 1–3, 5, 6, 8, 10, 12–16 och 18 §§ 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 dem enligt lagen.

Längsta tid som personuppgifter får behandlas

21 § Personuppgifter får inte behandlas under längre tid än vad som behövs med hänsyn till ändamålen med behandlingen.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om att personuppgifter får behandlas under endast viss tid eller fortsätta behandlas för arkivändamål av allmänt intresse eller för vetenskapliga, statistiska eller historiska ändamål.

Regeringen eller den myndighet som regeringen bestämmer får också besluta om sådan behandling i ett enskilt fall.

Paragrafen reglerar längsta tid som personuppgifter får behandlas. Övervägandena finns i avsnitt 8.6.

Enligt *första stycket* får personuppgifter inte behandlas under längre tid än vad som behövs med hänsyn till ändamålen med behandlingen. Att det inte längre finns behov av att behandla personuppgiften enligt ett visst ändamål medför inte att behandlingen av den måste upphöra för alla ändamål samtidigt. Det förhållandet att personuppgiften fortfarande behövs för ett visst ändamål innebär dock inte att uppgiften får fortsätta att behandlas för alla ändamål lika länge. 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.

Stycket 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 en mer övergripande nivå och i större utsträckning utgå från sannolikheten av att personuppgifterna kan komma att behövas i verksamheten än en reell bedömning av den enskilda uppgiften.

Stycket 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 upplysningsbestämmelse om att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter om att personuppgifter får behandlas under endast viss tid eller fortsätta behandlas för arkivändamål av allmänt intresse eller för vetenskapliga, statistiska eller historiska ändamål.

Enligt *tredje stycket* får regeringen eller den myndighet som regeringen bestämmer också besluta om sådan behandling i ett enskilt fall.

Överföring av personuppgifter till en mottagare utomlands

22 § Personuppgifter som behandlas med stöd av denna lag får föras över till ett annat land eller en internationell organisation 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 med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om att överföring får ske även i andra fall om det är nödvändigt för verksamheten vid Försvarsmakten.

Regeringen får också besluta om sådan överföring i ett enskilt fall.

Paragrafen reglerar överföring av personuppgifter till en mottagare utomlands. Övervägandena finns i avsnitt 10.5. Rubriken närmast före paragrafen utformas enligt *Lagrådets* förslag.

Enligt *första stycket* får personuppgifter som behandlas med stöd av lagen föras över till ett annat land eller en internationell organisation 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.

Huruvida en överföring av personuppgifter ska ske eller inte måste i sin helhet avgöras efter en sekretessprövning och försvars- och säkerhetspolitiska överväganden.

I *andra stycket* finns en upplysningsbestämmelse om att regeringen kan meddela föreskrifter om att överföring får ske även i andra fall om det är nödvändigt för verksamheten vid Försvarsmakten. En tänkbar situation är verksamhet som inte ingår i Försvarsmaktens internationella försvars- och säkerhetssamarbete. Det kan t.ex. vara nödvändigt för Försvarsmakten att överföra personuppgifter inom ramen för myndighetens administrativa verksamhet.

Enligt *tredje stycket* får regeringen också besluta om sådan överföring i ett enskilt fall.

Utlämnande av personuppgifter

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

Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om begränsning av möjligheten att lämna ut personuppgifter elektroniskt på annat sätt än genom direktåtkomst.

Paragrafen reglerar utlämnande av personuppgifter. Övervägandena finns i avsnitt 10.2.

Enligt *första stycket* får personuppgifter lämnas ut elektroniskt på annat sätt än genom direktåtkomst, 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. Typiskt sett kan det inte anses vara olämpligt att lämna ut uppgifter elektroniskt till en myndighet.

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 Försvarsmakten 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 det sättet. Vid prövningen av om personuppgifter bör lämnas ut elektroniskt bör även informationssäkerheten, dvs. säkerheten hos mottagaren, vägas in.

Regeringen kan enligt *andra stycket* meddela föreskrifter som begränsar möjligheten att lämna ut personuppgifter elektroniskt på annat sätt än genom direktåtkomst.

3 kap. Gemensamt tillgängliga personuppgifter

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. Med att göra personuppgifter gemensamt tillgängliga avses inte att endast ett fåtal personer får tillgång till uppgifterna.

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

Regeringen eller den myndighet som regeringen bestämmer får också besluta om uppgiftssamlingar i ett enskilt fall.

Paragrafen reglerar personuppgifter som får göras gemensamt tillgängliga. Övervägandena finns i avsnitt 9.

I *första stycket* anges genom en hänvisning till i lagen angivna ändamål vilka personuppgifter som får göras gemensamt tillgängliga. Vidare anges att med att göra personuppgifter gemensamt tillgängliga avses inte att endast ett fåtal personer får tillgång till uppgifterna. 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.

I *andra stycket* finns en upplysningsbestämmelse om att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter om vilka uppgiftssamlingar som får finnas och vilka uppgifter som får behandlas i respektive uppgiftssamling.

Enligt *tredje stycket* får regeringen eller den myndighet som regeringen bestämmer också besluta om uppgiftssamlingar i ett enskilt fall.

2 § Totalförsvarets plikt- och prövningsverk får medges direktåtkomst till personuppgifter som rör Försvarsmaktens personalförsörjning och krigsorganisation och som har gjorts gemensamt tillgängliga inom Försvarsmakten.

Totalförsvarets plikt- och prövningsverk har rätt att vid direktåtkomst ta del av de personuppgifter som omfattas av åtkomsten.

Paragrafen reglerar Totalförsvarets plikt- och prövningsverks direktåtkomst till vissa personuppgifter som Försvarsmakten behandlar. Övervägandena finns i avsnitt 10.3.1. Paragrafen utformas efter synpunkter från *Lagrådet*.

Enligt *första stycket* får Totalförsvarets plikt- och prövningsverk medges direktåtkomst till personuppgifter som rör Försvarsmaktens personalförsörjning och krigsorganisation och som har gjorts gemensamt tillgängliga inom Försvarsmakten. Genom direktåtkomst underlättas informationsutbytet om totalförsvarspliktiga mellan myndigheterna. Det ankommer på Försvarsmakten att avgöra om direktåtkomst ska medges.

I *andra stycket* finns en sekretessbrytande bestämmelse som anger att Totalförsvarets plikt- och prövningsverk har rätt att vid direktåtkomst ta del av de personuppgifter som omfattas av åtkomsten.

3 § Säkerhetspolisen och Försvarets radioanstalt får medges direktåtkomst till personuppgifter som utgör bearbetningsunderlag och analysresultat inom försvarsunderrättelseverksamheten och som finns i uppgiftssamlingar.

Säkerhetspolisen och Försvarets radioanstalt har rätt att vid direktåtkomst ta del av de personuppgifter som omfattas av åtkomsten.

Paragrafen reglerar Säkerhetspolisens och Försvarets radioanstalts direktåtkomst till vissa personuppgifter som Försvarsmaktens behandlar. Övervägandena finns i avsnitt 10.3.1.

I *första stycket* anges att Säkerhetspolisen och Försvarets radioanstalt får medges direktåtkomst till uppgifter som utgör bearbetningsunderlag och analysresultat inom försvarsunderrättelseverksamheten och som finns i uppgiftssamlingar. Bearbetningsunderlag och analysresultat består av information som ännu inte har bearbetats till underrättelserapporter. Det ankommer på Försvarsmakten att avgöra om direktåtkomst ska medges.

Andra stycket innehåller en sekretessbrytande bestämmelse som möjliggör för myndigheterna att vid direktåtkomst få ta del av uppgifter som omfattas av sekretess.

4 § 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 med stöd av 2 kap. 3 § och som finns i uppgiftssamlingar.

Första stycket gäller enbart i den utsträckning som sådan direktåtkomst följer av lag eller förordning eller om regeringen har beslutat om den i ett enskilt fall.

I paragrafen regleras Försvarsmaktens möjlighet att medge en utländsk underrättelse- eller säkerhetstjänst direktåtkomst till vissa personuppgifter. Övervägandena finns i avsnitt 10.3.2.

Av *första stycket* framgår att en utländsk underrättelse- eller säkerhetstjänst får medges direktåtkomst till personuppgifter som

behandlas med stöd av 2 kap. 3 § och som finns i uppgiftssamlingar, om det behövs för samarbetet mot terrorism eller vid svenskt deltagande i annat internationellt underrättelse- och säkerhetssamarbete. Möjligheten att dela information genom direktåtkomst begränsas till utländska underrättelse- och säkerhetstjänster. Direktåtkomst får endast medges till personuppgifter som behandlas i Försvarsmaktens försvarsunderrättelseverksamhet och som finns i uppgiftssamlingar.

Innan direktåtkomst medges måste Försvarsmakten avgöra om det finns sakliga skäl att låta en viss utländsk underrättelse- eller säkerhetstjänst få ta del av personuppgifterna, dvs. om det finns behov av att lämna ut uppgifterna för att främja bekämpningen av terrorism eller andra svenska intressen. Innan personuppgifterna lämnas ut genom direktåtkomst ska Försvarsmakten dessutom bedöma om det finns rättsliga förutsättningar att lämna ut dem till en utländsk mottagare, bl.a. med beaktande av sekretess.

Enligt *andra stycket* gäller första stycket endast i den utsträckning som sådan direktåtkomst följer av lag eller förordning eller om regeringen har beslutat om den i ett enskilt fall.

5 § 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 § och som finns i uppgiftssamlingar.

Första stycket gäller enbart i den utsträckning som sådan direktåtkomst följer av lag eller förordning eller om regeringen har beslutat om den i ett enskilt fall.

I paragrafen regleras Försvarsmaktens möjlighet att medge en utländsk underrättelse- eller säkerhetstjänst direktåtkomst till vissa personuppgifter i Försvarsmaktens militära säkerhetstjänst. Övervägandena finns i avsnitt 10.3.2.

Av *första stycket* framgår att en utländsk underrättelse- eller säkerhetstjänst får medges direktåtkomst till personuppgifter som behandlas med stöd av 2 kap. 5 § och som finns i uppgiftssamlingar, om det behövs för samarbetet mot säkerhetshotande verksamhet som riktas mot Försvarsmakten och dess säkerhetsintressen. Möjligheten att dela information genom direktåtkomst begränsas till utländska underrättelse- och säkerhetstjänster. Direktåtkomst får endast medges till personuppgifter som behandlas i Försvarsmaktens militära säkerhetstjänst och som finns i uppgiftssamlingar.

Innan direktåtkomst medges måste Försvarsmakten avgöra om det finns sakliga skäl att låta en viss utländsk underrättelse- eller säkerhetstjänst få ta del av personuppgifterna, dvs. om det finns behov av att lämna ut uppgifterna för att stärka skyddet för Försvarsmakten och dess säkerhetsintressen i förhållande till säkerhetshotande verksamhet. Innan personuppgifterna lämnas ut genom direktåtkomst ska Försvarsmakten dessutom bedöma om det finns rättsliga förutsättningar att lämna ut dem till en utländsk mottagare, bl.a. med beaktande av sekretess.

Enligt *andra stycket* gäller första stycket endast i den utsträckning som sådan direktåtkomst följer av lag eller förordning eller om regeringen har beslutat om den i ett enskilt fall.

6 § Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om direktåtkomst till gemensamt tillgängliga uppgifter eller uppgiftssamlingar i andra fall än de som anges i 2–5 §§.

Regeringen får också besluta om detta i ett enskilt fall.

Paragrafen reglerar direktåtkomst i andra fall. Övervägandena finns i avsnitten 10.3.1 och 10.3.2.

Första stycket innehåller en upplysningsbestämmelse om att regeringen kan meddela föreskrifter om att andra än de som anges i 2–5 §§ får ha direktåtkomst till gemensamt tillgängliga uppgifter eller uppgiftssamlingar.

Enligt *andra stycket* får regeringen också besluta om detta i ett enskilt fall.

Enligt regeringsformen får skyddet gentemot det allmänna mot vissa fall av betydande intrång i den personliga integriteten begränsas enbart genom lag (2 kap. 6 § andra stycket och 20–21 §§ regeringsformen). Regeringens möjlighet att meddela föreskrifter är således begränsad.

Omfattningen av direktåtkomsten

7 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om omfattningen av direktåtkomsten och om behörighet och säkerhet vid sådan åtkomst.

Regeringen får också besluta om detta i ett enskilt fall.

Paragrafen reglerar omfattningen av direktåtkomsten. Övervägandena finns i avsnitten 10.3.1 och 10.3.2.

Första stycket innehåller en upplysningsbestämmelse om att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter om omfattningen av direktåtkomsten, och om behörighet och säkerhet vid sådan åtkomst.

Enligt *andra stycket* får regeringen också får besluta om detta i ett enskilt fall.

4 kap. Skyldigheter 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 att de registrerades rättigheter skyddas.

Paragrafen reglerar åtgärder för att säkerställa författningsenlig behandling. Övervägandena finns i avsnitt 11.3.1.

Tekniska och organisatoriska åtgärder för att skydda personuppgifterna regleras i 3 §.

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. Åtgärder som vidtas för att visa att behandlingen är författningsenligt kan t.ex. vara dokumentation av it-system, behandlingar och vidtagna åtgärder samt teknisk spårbarhet genom loggning och logguppföljning. 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 § Tillgången till personuppgifter ska begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter.

Paragrafen reglerar den interna tillgången till personuppgifter för dem som arbetar vid Försvarsmakten. Övervägandena finns i avsnitt 11.3.2.

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.

Paragrafen gäller enligt 10 § även för personuppgiftsbiträden som Försvarsmakten anlitar.

Säkerheten för personuppgifter

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

I paragrafen regleras säkerheten för personuppgifter. Övervägandena finns i avsnitt 11.3.2.

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, som illustrerar vad skyddsåtgärderna ska åstadkomma, 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.

Tänkbara exempel på organisatoriska skyddsåtgärder kan vara 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.

Paragrafen gäller enligt 10 § även för personuppgiftsbiträden som Försvarsmakten anlitar.

Dataskyddsombud

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

Paragrafen reglerar skyldighet att utse dataskyddsombud. Övervägandena finns i avsnitt 11.4.

Enligt paragrafen ska ett eller flera dataskyddsombud utses. Dataskyddsombudet ska vara anställt hos Försvarsmakten. Försvarsmakten ska anmäla till tillsynsmyndigheten när dataskyddsombud utses och entledigas.

5 § Ett dataskyddsombud 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. vara kontaktpunkt för enskilda i frågor som rör Försvarsmaktens behandling av personuppgifter, och
4. vid behov söka vägledning av tillsynsmyndigheten.

I paragrafen anges vilka uppgifter ett dataskyddsombud ska utföra. Övervägandena finns i avsnitt 11.4.

Enligt *punkten 1* ska ett dataskyddsombud självständigt 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.

Dataskyddsombudet bör framför allt granska den praktiska hanteringen av personuppgifter. Därutöver bör ombudet 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 ett 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. Ombudet förutsätts också ha goda kunskaper om regelverket om personuppgiftsbehandling.

I *punkten 2* anges att ett dataskyddsombud ska informera och ge råd till Försvarsmakten och till dem som behandlar personuppgifter under myndighetens ledning om deras skyldigheter vid sådan behandling. Det handlar främst om att göra Försvarsmakten 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 dataskyddsombudet ska tala om för Försvarsmakten och medarbetarna hur de ska behandla personuppgifter i enskilda fall.

Ett dataskyddsombud ska vara kontaktpunkt för enskilda i frågor som rör behandling av personuppgifter, vilket anges i *punkten 3*.

Enligt *punkten 4* ska ett dataskyddsombud vid behov söka vägledning av tillsynsmyndigheten. Det innebär att ombudet vid tveksamheter av olika slag bör fråga tillsynsmyndigheten om råd.

Ett dataskyddsombud behöver inte uteslutande utföra enbart de arbetsuppgifter som anges i paragrafen. Arbetet som dataskyddsombud kan kombineras med andra arbetsuppgifter, så länge de inte kommer i konflikt med uppdraget som dataskyddsombud.

Personuppgiftsbiträden

6 § 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 registrerades rättigheter.

Paragrafen reglerar anlitande av personuppgiftsbiträden. Övervägandena finns i avsnitt 11.5.2.

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. Av paragrafen följer 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 undersöka hur biträdet kommer att behandla uppgifterna tekniskt, hur arbetet är organiserat och vilket skydd personuppgifterna kommer att ha.

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

Paragrafen reglerar förhållandet mellan Försvarsmakten och personuppgiftsbiträden. Övervägandena finns i avsnitt 11.5.2.

Av paragrafen följer att 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 ingår i samma juridiska person – staten, i rättslig mening inte kan ingå bindande avtal med varandra får de ingå en skriftlig överenskommelse som reglerar behandlingen om en myndighet agerar personuppgiftsbiträde åt en annan.

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

Paragrafen reglerar möjligheten för ett personuppgiftsbiträde att anlita ett annat personuppgiftsbiträde. Övervägandena finns i avsnitt 11.5.2.

Enligt paragrafen får ett personuppgiftsbiträde inte anlita ett annat personuppgiftsbiträde, ett s.k. underbiträde, utan skriftligt tillstånd från Försvarsmakten. Ett sådant tillstånd kan gälla personuppgiftsbiträdets rätt att anlita underbiträden generellt eller i en specifik situation. Syftet med paragrafen är att Försvarsmakten ska känna till vilka personuppgiftsbiträden som behandlar personuppgifter för myndighetens räkning.

9 § 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 reglerar behandling av personuppgifter hos ett personuppgiftsbiträde. Övervägandena finns i avsnitt 11.5.3.

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 bestämmelser i annan lagstiftning som anger att personuppgiftsbiträdet är skyldigt 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.

10 § Försvarsmaktens skyldigheter enligt 2 och 3 §§ gäller även för personuppgiftsbiträden som Försvarsmakten anlitar.

Paragrafen kopplar Försvarsmaktens skyldigheter i egenskap av personuppgiftsansvarig till att gälla även för personuppgiftsbiträden. Övervägandena finns i avsnitt 11.5.4.

Att personuppgiftsbiträden åläggs vissa skyldigheter fråntar inte Försvarsmakten dess ansvar som personuppgiftsansvarig. 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.

Vad som närmare gäller för ett personuppgiftsbiträde framgår av författningskommentaren till 2 och 3 §§.

5 kap. Enskildas rättigheter

Rätten till information

Allmän information

1 § Försvarsmakten ska göra följande information allmänt tillgänglig:

1. myndighetens identitet och kontaktuppgifter,
2. uppgifter om dataskyddsombudet,
3. kategorier av ändamål för behandlingen av personuppgifter,
4. rätten enligt 3 § att begära att få information om behandlingen av personuppgifter och att få del av dem, och
5. rätten att begära rättelse, radering eller begränsning av behandlingen enligt 6 §.

Paragrafen reglerar krav på att göra viss information allmänt tillgänglig. Övervägandena finns i avsnitt 12.1.1.

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. 4 § skyldig att utse ett eller flera 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.

Kategorier av ändamål för behandlingen av personuppgifter ska framgå, vilket anges i *punkten 3*. Det är inte ändamålen med behandlingen av personuppgifter i enskilda fall som avses utan för vilka kategorier av ändamål som myndigheten behandlar personuppgifter. Kategorier av ändamål kan t.ex. vara underrättelsearbete, säkerhetsskyddsarbete och personaladministrativa åtgärder.

Enligt *punkterna 4* och *5* ska Försvarsmakten 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 personuppgifterna samlas in från den som uppgifterna avser

2 § Om personuppgifter samlas in från den som uppgifterna avser ska Försvarsmakten, när myndigheten får personuppgifterna, på eget initiativ lämna följande information till den registrerade:

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

Paragrafen reglerar den information som Försvarsmakten på eget initiativ ska lämna om personuppgifterna samlas in från den som uppgifterna avser. Övervägandena finns i avsnitt 12.1.2.

Enligt paragrafen ska Försvarsmakten informera om att det är Försvarsmakten som är ansvarig för personuppgiftsbehandlingen (*punkten 1*), upplysa om ändamålen med behandlingen (*punkten 2*) samt lämna all övrig information som behövs för att den registrerade ska kunna ta till vara sina rättigheter i samband med behandlingen, såsom information om uppgifternas mottagare, om skyldighet att lämna uppgifter och om rätten att ansöka om information och få rättelse (*punkten 3*). Informationsskyldigheten förutsätter att personuppgifter samlas in från den registrerade 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 huruvida personuppgifter som rör honom eller henne behandlas. Om sådana uppgifter behandlas ska sökanden få del av dem och få följande skriftliga information:

1. vilka personuppgifter om den sökande som behandlas,
2. varifrån personuppgifterna kommer,
3. ändamålen med behandlingen,
4. mottagare eller kategorier av mottagare av personuppgifterna, även i annat land eller internationella organisationer,
5. hur länge personuppgifterna får behandlas eller, om det inte är möjligt att ange, kriterierna för att fastställa det, och
6. rätten att begära rättelse, radering eller begränsning av behandlingen enligt 6 §.

Ett utlämnande av personuppgifter enligt första stycket behöver inte omfatta sådana 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 om information enligt första stycket ska göras skriftligen hos Försvarsmakten och vara undertecknad av den sökande själv. Informationen 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 information som ska lämnas efter begäran. Övervägandena finns i avsnitt 12.1.2.

I *första stycket 1–6* anges vilken skriftlig information sökanden kan få del av.

Enligt *första stycket 1* ska i den skriftliga informationen anges vilka personuppgifter om den sökande som behandlas.

Enligt *första stycket 2* ska anges varifrån personuppgifterna kommer.

Enligt *första stycket 3* ska ändamålen med behandlingen anges.

Enligt *första stycket 4* ska mottagare eller kategorier av mottagare av personuppgifterna, även i annat land eller internationella organisationer, anges.

Enligt *första stycket 5* ska det anges hur länge personuppgifterna får behandlas eller, om det inte är möjligt att ange, kriterierna för att fastställa det.

Enligt *första stycket 6* ska rätten att begära rättelse, radering eller begränsning av behandlingen enligt 6 § anges.

Av *andra stycket* följer att sådana personuppgifter som sökanden har tagit del av som utgångspunkt inte omfattas av skyldigheten att lämna ut uppgifterna. Sökanden ska dock informeras om att personuppgifterna i fråga behandlas.

Av *tredje stycket* framgår kraven på en begäran om information.

Begränsning av rätten till information

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

Om det gäller sekretess är Försvarsmakten inte skyldig att redovisa skälen för ett beslut enligt första stycket eller ett beslut i fråga om rättelse, radering eller begränsning av behandlingen enligt 6 §.

I paragrafen regleras begränsningar av rätten till information. Övervägandena finns i avsnitt 12.2.

Många uppgifter som behandlas i Försvarsmaktens olika verksamheter omfattas av bl.a. 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 registrerade.

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

Informationsskyldigheten gäller dock om uppgifterna

1. har lämnats ut till tredje part, med undantag för en myndighet som med stöd av författning utövar tillsyn, kontroll eller revision,
2. behandlas enbart för statistiska ändamål eller arkivändamål av allmänt intresse, eller
3. har behandlats under längre tid än ett år i löpande text som inte har fått sin slutliga utformning.

I paragrafen regleras vissa undantag från informationsskyldigheten för personuppgifter i viss typ av text. Övervägandena finns i avsnitt 12.2.

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 en minnesanteckning 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 tillför ärendet något i sak.

Av *andra stycket* framgår att undantaget från informationsskyldigheten enligt första stycket 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. Enligt *andra stycket 1* gäller undantaget inte om personuppgifterna har lämnats ut till tredje part, såvida det inte är fråga om en myndighet som med stöd av författning utövar tillsyn, kontroll eller revision. Det är den version av uppgifterna i t.ex. utkastet som lämnades till tredje part som informationsskyldigheten omfattar, även om utkastet därefter har ändrats.

Undantaget från informationsskyldigheten gäller enligt *andra stycket 2* inte heller om personuppgifterna behandlas enbart för statistiska ändamål eller arkivändamål av allmänt intresse. Om ett ärende har avslutats och utkastet eller minnesanteckningen har arkiverats eller om handlingarna endast används vid statistikproduktion ska alltså information om behandlingen av personuppgifterna lämnas ut. Avslutningsvis gäller undantaget inte heller för löpande text som inte har fått sin slutliga utformning, om personuppgifterna har behandlats under längre tid än ett år, vilket framgår av *andra stycket 3*.

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 statistiska 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 registrerade snarast rätta, radera eller begränsa behandlingen av sådana personuppgifter som inte har behandlats i enlighet med denna lag eller föreskrifter som har meddelats med stöd av lagen.

Om uppgifterna har lämnats ut till tredje part ska denne underrättas om en åtgärd enligt första stycket, om den registrerade begär det eller om en mera betydande skada eller olägenhet för den registrerade 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.

I paragrafen, som utformas delvis enligt *Lagrådets* förslag, regleras rätten till rättelse, radering eller begränsning av behandlingen av personuppgifter. Övervägandena finns i avsnitt 12.3.

Försvarsmakten ska enligt *första stycket* på begäran av den registrerade snarast rätta, radera eller begränsa behandlingen av sådana personuppgifter som inte har behandlats i enlighet med denna lag eller föreskrifter som har meddelats med stöd av lagen. Begäran kan göras formlöst.

Kravet på att en åtgärd i form av rättelse, radering eller begränsning ska vidtas snarast innebär att Försvarsmakten skyndsamt ska utreda frågan och, om det finns skäl för det, så fort som möjligt genomföra åtgärden.

Begränsning av behandlingen av personuppgifter kan komma i fråga om den registrerade bestrider att personuppgifterna är riktiga, men det inte är möjligt att fastställa om så är fallet. En felaktig personuppgift ska rättas snarast möjligt. Om Försvarsmaktens utredning om den omstridda personuppgiften inte kan slutföras tillräckligt snabbt kan behandlingen behöva begränsas under utredningstiden. Har behandlingen av en personuppgift begränsats får uppgiften som utgångspunkt inte längre behandlas av Försvarsmakten, utom för de ändamål för vilka behandlingen begränsades. Uppgiften får dock lämnas ut med stöd av 2 kap. tryckfrihetsförordningen.

Försvarsmakten ska vidta åtgärder som visar att behandlingen av en viss personuppgift har begränsats. En sådan åtgärd kan vara att föra över uppgiften från det datasystem där den behandlas, t.ex. myndighetens verksamhetssystem, till ett arkivsystem. Andra åtgärder kan vara att göra personuppgiften oåtkomlig genom en teknisk begränsning eller annan inskränkning av tillgången till uppgiften. När utredningen om personuppgiften är avslutad ska begränsningen av behandlingen upphöra. Då ska personuppgiften antingen rättas eller fortsätta att behandlas som tidigare.

Försvarsmakten är enligt *andra stycket* skyldig att underrätta tredje part om en korrigering, om den registrerade 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 part 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.

Avgiftsfri information

7 § Information enligt 1 och 2 §§ och information och uppgifter enligt 3 § ska lämnas utan avgift.

Paragrafen reglerar avgiftsfri information. Övervägandena finns i avsnitten 12.1.1 och 12.1.2.

Enligt paragrafen ska information enligt 1 och 2 §§ och information och uppgifter enligt 3 § lämnas utan avgift.

6 kap. Tillsyn

Tillsyn över personuppgiftsbehandlingen

1 § Den myndighet som regeringen bestämmer utövar tillsyn över Försvarsmaktens behandling av personuppgifter enligt denna lag, enligt föreskrifter som har meddelats i anslutning till lagen och enligt beslut med stöd av lagen.

Tillsynsmyndigheten ska, när det är motiverat, ge råd och stöd till Försvarsmakten och personuppgiftsbiträden i frågor som gäller deras skyldigheter enligt lag eller annan författning.

I paragrafen, som utformas i linje med *Lagrådets* förslag, regleras tillsyn över personuppgiftsbehandlingen. Övervägandena finns i avsnitt 13.2.

Enligt *första stycket* ska tillsynsmyndigheten utöva tillsyn över Försvarsmaktens behandling av personuppgifter enligt lagen, enligt föreskrifter som har meddelats i anslutning till lagen och enligt beslut med stöd av lagen. 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 utomstående 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 har meddelats i anslutning till lagen.

Enligt *andra stycket* ska tillsynsmyndigheten, när det är motiverat, ge råd och stöd till Försvarsmakten och personuppgiftsbiträden i frågor som gäller deras skyldigheter enligt lag eller annan författning. 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 motiverat. Rådgivningen och stödet ska avse Försvarsmaktens och personuppgiftsbiträdens skyldigheter. Stycket innebär således inte någon rätt för Försvarsmakten eller personuppgiftsbiträden att avkräva tillsynsmyndigheten råd i en konkret fråga.

Tillsynsmyndighetens befogenheter

Undersökningsbefogenheter

2 § Tillsynsmyndigheten har rätt att av Försvarsmakten eller av 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. den hjälp och annan information som behövs för tillsynen.

I paragrafen regleras tillsynsmyndighetens undersökningsbefogenheter. Övervägandena finns i avsnitt 13.3.1.

Enligt *punkten 1* har tillsynsmyndigheten rätt att för sin tillsyn från Försvarsmakten och ett personuppgiftsbiträde få tillgång till personuppgifter som behandlas. Det innebär att Försvarsmakten eller personuppgiftsbiträdet ska lämna de begärda uppgifterna även om det kräver viss efterforskning.

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 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 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. Punkten 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 motverka den risken.

Tillsynsmyndigheten får besluta om en skriftlig varning, om en planerad behandling av personuppgifter riskerar att strida mot lag eller annan författning.

Detsamma gäller om en pågående behandling riskerar att strida mot lag eller annan författning.

Paragrafen reglerar tillsynsmyndighetens befogenheter i det förebyggande arbetet. Övervägandena finns i avsnitt 13.3.2.

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 motverka risken genom råd, rekommendationer och påpekanden. Rådgivning kan avse såväl formella som informella samråd. De befogenheter som anges i stycket får i vissa fall även användas i korrigerande syfte, vilket framgår av 4 § första stycket 1.

Enligt *andra stycket* får tillsynsmyndigheten besluta om en skriftlig varning, om en planerad behandling riskerar att strida mot lag eller annan författning. 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 beslutar om en varning. Av beslutet ska framgå varför tillsynsmyndigheten bedömt att behandlingen inte kommer att vara författningsenlig. Ett beslut om varning har inte några omedelbara rättsverkningar, men den som får en varning förväntas rätta sig efter den.

Varning får också beslutas om en pågående behandling riskerar att strida mot 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 på annat sätt 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 för att fullgöra andra skyldigheter, eller
2. besluta att förelägga Försvarsmakten eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsenlig eller för att fullgöra andra skyldigheter.

Av ett beslut om föreläggande ska det framgå när föreläggandet senast ska ha följts och, om det är lämpligt, vilka åtgärder som ska vidtas.

I paragrafen, som utformas enligt förslag och efter synpunkter från *Lagrådet*, regleras tillsynsmyndighetens korrigerande befogenheter. Övervägandena finns i avsnitt 13.3.3.

Tillsynsmyndigheten har möjlighet att successivt använda olika medel och på så sätt öka 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 på annat sätt 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 1* får tillsynsmyndigheten använda de förebyggande befogenheter som regleras i 3 § första stycket för att försöka förmå Försvarsmakten eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsenlig eller för att fullgöra andra skyldigheter.

Enligt *första stycket 2* får tillsynsmyndigheten besluta att förelägga Försvarsmakten eller personuppgiftsbiträdet att vidta åtgärder för att viss behandling av personuppgifter ska bli författningsenlig eller för att de ska fullgöra andra skyldigheter.

Av *andra stycket* framgår att det av ett beslut om föreläggande alltid ska framgå när föreläggandet senast ska ha följts 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 registrerade för den skada och kränkning av den personliga integriteten som orsakats av behandling av personuppgifter i strid med denna lag, föreskrifter som har meddelats i anslutning till lagen eller beslut med stöd av lagen.

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

I paragrafen regleras skadestånd. Övervägandena finns i avsnitt 14.3.2.

Av *första stycket* framgår att rätt till skadestånd kan uppkomma på grund av behandling i strid med bestämmelser i lagen, föreskrifter som har meddelats i anslutning till lagen eller beslut med stöd av lagen. För att den personuppgiftsansvarige ska bli ersättningsskyldig måste den registrerade bevisa att behandling av dennes personuppgifter stått i strid med bestämmelserna 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. Den praxis som finns om tillämpningen av bestämmelserna i den upphävda lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och

militära säkerhetstjänst och personuppgiftslagen om skadestånd är avsedd att vara vägledande.

Av *andra stycket* följer att ersättningsskyldigheten, i den utsträckning det är skäligt, kan jämkas om den personuppgiftsansvarige visar att felet inte berodde på denne.

Överklagande

Överklagande av Försvarsmaktens beslut

2 § Försvarsmaktens beslut enligt 5 kap. 2 och 3 §§ att inte lämna information och beslut enligt 5 kap. 6 § i fråga om rättelse, radering, begränsning av behandlingen eller underrättelse till tredje part, får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Paragrafen reglerar överklagande av Försvarsmaktens beslut. Övervägandena finns i avsnitt 14.4.1.

Enligt *första stycket* får Försvarsmaktens beslut enligt 5 kap. 2 och 3 §§ att inte lämna information och beslut enligt 5 kap. 6 § i fråga om rättelse, radering, begränsning av behandlingen eller underrättelse till tredje part överklagas till allmän förvaltningsdomstol. Uppräkningen är, som framgår av 4 §, uttömmande.

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.

Överklagande av tillsynsmyndighetens beslut

3 § Tillsynsmyndighetens beslut om föreläggande enligt 6 kap. 4 § första stycket 2 får överklagas till allmän förvaltningsdomstol. När ett beslut överklagas är tillsynsmyndigheten motpart i domstolen.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Paragrafen reglerar överklagande av tillsynsmyndighetens beslut. Övervägandena finns i avsnitt 14.4.2.

Enligt *första stycket* får tillsynsmyndighetens beslut om föreläggande enligt 6 kap. 4 § första stycket 2 överklagas till allmän förvaltningsdomstol. Det anges vidare att tillsynsmyndigheten är motpart i domstolen när ett beslut överklagas.

Enligt *andra stycket* krävs prövningstillstånd vid överklagande till kammarrätten.

Överklagandeförbud

4 § Andra beslut enligt denna lag än de som anges i 2 och 3 §§ får inte överklagas.

Paragrafen innehåller ett överklagandeförbud. Övervägandena finns i avsnitten 14.4.1 och 14.4.2.

Av paragrafen framgår att andra beslut enligt lagen än de som anges i 2 och 3 §§ inte får överklagas. Uppräkningen är uttömmande. Någon rätt att

med stöd av förvaltningslagen (2017:900) överklaga andra beslut av Försvarsmakten eller tillsynsmyndigheten enligt lagen finns alltså inte.

Ikraftträdande- och övergångsbestämmelser

1. Denna lag träder i kraft den 1 januari 2022.
2. Genom lagen upphävs lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst.
3. Äldre föreskrifter gäller fortfarande för överklagande av beslut som har meddelats före ikraftträdandet.

Ikraftträdande- och övergångsbestämmelserna behandlas i avsnitt 17.

Enligt *punkten 1* träder lagen i kraft den 1 januari 2022.

Genom *punkten 2* upphävs lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst.

Av *punkten 3* följer att äldre föreskrifter fortfarande gäller för överklagande av beslut som har meddelats före ikraftträdandet. Med äldre föreskrifter avses lagen om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst, förordningen (2007:260) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst, personuppgiftslagen (1998:204) och personuppgiftsförordningen (1998:1191).

19.2 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.

I paragrafen anges syftet med lagen. Övervägandena finns i avsnitt 6.3.

Enligt paragrafen är syftet med lagen 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. Lagen har alltså två syften och gäller för enbart fysiska personer. Det innebär att juridiska personer inte omfattas av lagen.

Lagens tillämpningsområde

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

I paragrafen regleras lagens tillämpningsområde. Övervägandena finns i avsnitt 6.4.2.

I paragrafen anges att lagen gäller vid behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet samt informationssäkerhetsverksamhet.

Försvarets radioanstalt bedriver försvarsunderrättelse- och utvecklingsverksamhet enligt lagen (2000:130) om försvarsunderrättelseverksamhet och lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet, och anslutande förordningar.

Av förordningen (2007:937) med instruktion för Försvarets radioanstalt framgår att Försvarets radioanstalt ska ha hög teknisk kompetens inom informationssäkerhetsområdet. Myndigheten ska även kunna lämna stöd inom detta område. Försvarets radioanstalt har vidare till uppgift enligt förordningen (2015:1053) om totalförsvar och höjd beredskap att tilldela säkra kryptografiska funktioner till ett antal civila myndigheter och organisationer.

All behandling av personuppgifter som Försvarets radioanstalt utför inom ramen för verksamheter som anges i paragrafen omfattas av lagen. För Försvarets radioanstalts övriga behandling av personuppgifter är EU:s dataskyddsförordning och dataskyddslagen (2018:218) tillämpliga.

I 2 kap. anges närmare de ändamål för vilka Försvarets radioanstalt får behandla personuppgifter.

3 § Lagen gäller vid sådan behandling av personuppgifter som är helt eller delvis automatiserad. Den gäller också personuppgifter som ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

Paragrafen preciserar lagens tillämpningsområde. Övervägandena finns i avsnitt 6.4.1.

Av paragrafen framgår att lagen gäller vid sådan behandling av personuppgifter som är helt eller delvis automatiserad och också personuppgifter som ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

När det gäller automatiserad behandling krävs det inte att personuppgifterna som behandlas finns i något som kan karaktäriseras som ett register eller att de annars är ordnade på visst sätt. Manuell behandling i t.ex. register omfattas av bestämmelsen om personuppgifterna är tillgängliga för sökning eller sammanställning enligt mer än ett kriterium. Uteslutande manuell behandling av personuppgifter som inte ingår i någon samling och inte heller är avsedda att ingå i en sådan, exempelvis handskrivna minnesanteckningar, faller däremot utanför tillämpningsområdet.

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

I paragrafen regleras förhållandet till EU:s dataskyddsförordning och lagen med kompletterande bestämmelser till EU:s dataskyddsförordning. Övervägandena finns i avsnitt 6.2.

Av paragrafen framgår att 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) och lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning inte gäller vid behandling av personuppgifter enligt lagen.

Ord och uttryck i lagen

5 § I denna lag används följande ord och uttryck.

Ord och uttryck	*Betydelse*
Behandling av personuppgifter	En åtgärd eller en 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 identifiering av personen i fråga.
Dataskyddsombud	En fysisk person som utses av den personuppgiftsansvarige för att självständigt kontrollera att personuppgifter behandlas författningsenligt och på ett korrekt sätt.
Genetiska uppgifter	Personuppgifter som rör en persons nedärvda eller förvärvade genetiska kännetecken och som framför allt härrör från analys av ett spår av eller ett biologiskt prov från personen i fråga.
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 behandlar personuppgifter för den personuppgiftsansvariges räkning.
Registrerad	Den fysiska person som personuppgiften gäller.
Tredje part	Någon annan än – den registrerade, – den 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.

I paragrafen definieras vissa ord och uttryck som används i lagen.

Behandling av personuppgifter

Uttrycket behandling av personuppgifter omfattar alla åtgärder som vidtas med sådana uppgifter. Uttrycket behandlas i avsnitt 6.5.

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

Biometri är en samlingsbenämning för sådan automatiserad teknik som syftar till att identifiera en person eller avgöra om en påstådd identitet är riktig. Uttrycket behandlas i avsnitt 6.5.

Den automatiserade tekniken 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 för närvarande 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 författningskommentaren till uttrycket genetiska uppgifter.

Av 2 kap. 14 § 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 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. Fotografier kan omfattas av regleringen om känsliga personuppgifter även på andra grunder, se författningskommentaren till 2 kap. 13 §.

Dataskyddsombud

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. Ordet behandlas i avsnitt 11.4.

Ett dataskyddsombud ska vara anställd hos den personuppgifts-ansvarige. Kravet på självständighet innebär att dataskyddsombud ska kunna utföra sina arbetsuppgifter på ett oberoende sätt. Ombuden förutsätts framför allt ha goda kunskaper om regelverket om personuppgiftsbehandling. Ombuden bör också ha sådan ställning i organisationen att det säkerställs att deras synpunkter och råd beaktas.

Genetiska uppgifter

Med uttrycket genetiska uppgifter avses personuppgifter som rör en persons nedärvda eller förvärvade genetiska kännetecken och som framför allt härrör från analys av ett spår av eller ett biologiskt prov från personen i fråga. Det är alltså fråga om all information som rör en persons nedärvda eller förvärvade genetiska kännetecken och som kan tas fram ur ett spår från människokroppen. Uttrycket behandlas i avsnitt 6.5.

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. Den dna-profil, som behandlas i ett 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 identifiering av personen i fråga.

Mottagare

Mottagare definieras som den till vilken personuppgifter lämnas ut, med undantag av en myndighet som med stöd av författning utövar tillsyn, kontroll eller revision. Ordet behandlas i avsnitt 6.5.

Undantaget omfattar bl.a. myndigheter som tar del av personuppgifter i sin tillsyn och kontroll av viss verksamhet, t.ex. Integritetsskyddsmyndigheten och Statens inspektion för försvarsunderrättelseverksamheten. Även andra myndigheter som utövar tillsyn, t.ex. Riksdagens ombudsmän (JO) och Justitiekanslern, omfattas av undantaget.

Personuppgift

Med personuppgift avses varje upplysning om en identifierad eller identifierbar fysisk person som är i livet. Ordet behandlas i avsnitt 6.5.

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.

Uppgifter om juridiska personer omfattas inte av definitionen.

Personuppgiftsansvarig

Personuppgiftsansvarig är enligt definitionen den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter. Ordet behandlas i avsnitt 11.1.

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

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. Ordet behandlas i avsnitt 11.5.1.

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.

Registrerad

Med registrerad avses den fysiska person som en personuppgift rör. Ordet behandlas i avsnitt 6.5.

Av definitionen av personuppgift framgår bl.a. att personen ska vara i livet.

Tredje part

Tredje part är någon annan än den registrerade, personuppgiftsansvarige, dataskyddsombudet, personuppgiftsbiträdet, och sådana personer som under den personuppgiftsansvarige eller personuppgiftsbiträdets direkta ansvar har rätt att behandla personuppgifter. Uttrycket behandlas i avsnitt 6.5.

Uppgiftssamling

Uppgiftssamling är en samling med uppgifter som med hjälp av automatiserad behandling är gemensamt tillgängliga. Ordet behandlas i avsnitt 6.5.

Avgörande för när automatiserat behandlade uppgifter ska anses ingå i en uppgiftssamling är att uppgifterna är gemensamt tillgängliga i Försvarets radioanstalt för de ändamål som ska styra behandlingen av uppgifter inom myndighetens försvarsunderrättelse- och utvecklingsverksamhet samt informationssäkerhetsverksamhet.

Personuppgiftsansvar

6 § Försvarets radioanstalt är personuppgiftsansvarig för all behandling av personuppgifter som myndigheten utför, som utförs under myndighetens ledning eller på dess vägnar.

Paragrafen reglerar personuppgiftsansvar. Övervägandena finns i avsnitt 11.1. Paragrafen utformas enligt *Lagrådets* förslag.

I *paragrafen* anges att Försvarets radioanstalt är personuppgiftsansvarig för all behandling av personuppgifter som myndigheten utför, som utförs under myndighetens ledning eller på dess vägnar. Den närmare innebörden av personuppgiftsansvaret framgår av övriga bestämmelser i lagen och föreskrifter som har meddelats i anslutning till lagen.

Personuppgiftsansvaret omfattar alltså all behandling av personuppgifter som utförs vid myndigheten. Det gäller både behandling som utförs genom en aktiv handling, t.ex. insamling eller sökning, och passiv behandling, t.ex. lagring. Ansvaret omfattar däremot inte sådan behandling som myndigheten utför i egenskap av personuppgiftsbiträde. Genom att ansvaret knyts till behandling som utförs under Försvarets radioanstalts ledning tydliggörs att det inte är myndigheten som utför personuppgiftsbehandlingen utan de anställda.

Försvarets radioanstalt är också ansvarig för den behandling av personuppgifter som utförs på myndighetens vägnar. Med det avses främst sådan behandling som Försvarets radioanstalt har uppdragit åt ett person-

uppgiftsbiträde att utföra. Försvarets radioanstalt kan uppdra åt ett biträde att utföra viss behandling av personuppgifter, men kan inte genom det avsäga sig personuppgiftsansvaret. Personuppgiftsansvaret sträcker sig då utanför Försvarets radioanstalts egen verksamhet. Personuppgiftsbiträdets behandling ska styras av skriftliga avtal eller andra skriftliga överenskommelser och får endast utföras enligt instruktioner från Försvarets radioanstalt, se författningskommentarerna till 4 kap. 7 och 9 §§.

Två eller flera personuppgiftsansvariga kan behandla samma personuppgifter samtidigt för olika ändamål, t.ex. om de har direktåtkomst till personuppgifter i samma system. Varje personuppgiftsansvarig är dock ansvarig för den behandling som utförs under dennes ledning eller på dennes vägnar.

2 kap. Behandling av personuppgifter

Grundläggande krav på behandlingen

Krav på ändamål

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

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

I paragrafen regleras grundläggande krav på behandlingen av personuppgifter i fråga om krav på ändamål. Övervägandena finns i avsnitt 7.1.

Enligt *första stycket* får personuppgifter bara behandlas för särskilda, uttryckligt angivna och berättigade ändamål. Det ställs alltså 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 Försvarets radioanstalts uppgifter enligt lag eller annan författning, eller ett enskilt beslut från regeringen. Detta innebär att ändamålen med en behandling av personuppgifter måste bestämmas redan när uppgifterna samlas in.

Av *andra stycket* framgår att personuppgifter inte får behandlas för något ändamål som är oförenligt med det ändamål som de ursprungligen behandlades för. Bestämmelsen ger uttryck för den generella s.k. finalitetsprincipen, dvs. att fortsatt behandling inte får ske för något ändamål som är oförenligt med det ändamål för vilket personuppgifterna ursprungligen behandlades. Vad som kan utgöra oförenliga ändamål måste avgöras i det enskilda fallet. Det innebär att den personuppgiftsansvarige under hela behandlingstiden måste hålla reda på för vilka ändamål varje personuppgift ursprungligen har behandlats för.

Försvarsunderrättelseverksamhet

2 § 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 anger de ändamål för vilka Försvarets radioanstalt får behandla personuppgifter i sin försvarsunderrättelseverksamhet. Övervägandena finns i avsnitt 7.3.1.

I paragrafen hänvisas till den verksamhet som ska bedrivas enligt lagen (2000:130) om försvarsunderrättelseverksamhet och lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet. 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 söka efter företeelser och hot som är okända men som antas existera.

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

Första stycket gäller endast om inte något annat följer av denna lag eller en förordning som regeringen har meddelat i anslutning till lagen.

Paragrafen kompletterar 2 § när det är tillåtet att behandla personuppgifter i Försvarets radioanstalts försvarsunderrättelseverksamhet. Övervägandena finns i avsnitt 7.3.1.

I *första stycket* anges att de personuppgifter som Försvarets radioanstalt har fått tillgång till i sin försvarsunderrättelseverksamhet även fortsättningsvis får behandlas i den verksamheten, om det behövs för att fullgöra den. Härigenom möjliggörs en fortsatt behandling av personuppgifter som finns inom Försvarets radioanstalts försvarsunderrättelseverksamhet, under förutsättning att en sådan behandling är nödvändig för att fullgöra den verksamheten. Härigenom möjliggörs en behandling som inte alltid direkt kan hänföras till regeringens vid varje tidpunkt gällande inriktning av försvarsunderrättelseverksamheten. Det är av grundläggande betydelse att Försvarets radioanstalt kan behandla äldre information, inbegripet personuppgifter, för att kunna förstå och bedöma den underrättelsemässiga relevansen av sådant som sker i dagsläget.

Första stycket gäller endast om inte något annat följer av lag eller förordning som regeringen har meddelat i anslutning till lagen. Detta framgår av *andra stycket*.

4 § Personuppgifter som behandlas med stöd av 2 och 3 §§ 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 om försvarsunderrättelseverksamhet och lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet,
3. i utvecklingsverksamheten för de ändamål som anges i 5 §,
4. i informationssäkerhetsverksamheten för de ändamål som anges i 7 §, eller

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

Paragrafen reglerar vidarebehandling av personuppgifter inom försvarsunderrättelseverksamheten. Övervägandena finns i avsnitt 7.3.1.

I *punkten 1* anges att Försvarets radioanstalt får behandla personuppgifter för att tillhandahålla information som behövs hos berörda myndigheter som avses i 2 § första stycket lagen (2000:130) om försvarsunderrättelseverksamhet. Av den bestämmelsen följer att försvarsunderrättelsemyndigheterna ska rapportera underrättelser till berörda myndigheter. Vilken den enskilda mottagande myndigheten är beror på det enskilda fallet.

Enligt *punkten 2* får Försvarets radioanstalt vidarebehandla personuppgifter med anledning av samarbete med andra länder och internationella organisationer enligt lagen om försvarsunderrättelseverksamhet och lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet. Punkten innebär ett uttryckligt stöd för den behandling av personuppgifter som Försvarets radioanstalt utför i sitt internationella samarbete inom försvarsunderrättelseverksamheten och signalspaning i sådan verksamhet.

Av *punkten 3* följer att Försvarets radioanstalt även får vidarebehandla personuppgifterna om det är nödvändigt att tillhandahålla information som behövs i utvecklingsverksamheten för de ändamål som anges i 5 §.

Genom *punkten 4* får vidarebehandling av personuppgifterna även ske i Försvarets radioanstalts informationssäkerhetsverksamhet för de ändamål som anges i 7 §.

Enligt *punkten 5* får Försvarets radioanstalt vidarebehandla personuppgifterna om det är nödvändigt för att tillhandahålla information som behövs för att biträda andra myndigheter i den utsträckning det följer av lag eller förordning eller om regeringen har beslutat om det i ett enskilt fall.

Utvecklingsverksamhet

5 § 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 reglerar de ändamål för vilka Försvarets radioanstalt får behandla personuppgifter i sin utvecklingsverksamhet. Övervägandena finns i avsnitt 7.3.2.

Försvarets radioanstalt får behandla personuppgifter för att följa förändringar i signalmiljön i omvärlden, den tekniska utvecklingen och signalskyddet (*punkten 1*) och fortlöpande utveckla den teknik och metodik som behövs för att bedriva verksamheten (*punkten 2*). I samtliga fall krävs att behandlingen ska vara nödvändig för Försvarets radioanstalts försvarsunderrättelseverksamhet.

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

1. med anledning av samverkan med annan i fråga om 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 2 och 3 §§,
4. i informationssäkerhetsverksamheten för de ändamål som anges i 7 §, eller
5. för att biträda andra myndigheter i den utsträckning det följer av lag eller förordning eller om regeringen har beslutat om det i ett enskilt fall.

Paragrafen reglerar vidarebehandling av personuppgifter som har behandlats inom utvecklingsverksamheten. Övervägandena finns i avsnitt 7.3.2.

Enligt *punkten 1* får Försvarets radioanstalt även behandla de aktuella personuppgifterna för att tillhandahålla information som behövs med anledning av samverkan med annan i fråga om utvecklingsverksamhet. Sådan samverkan kan ske med andra myndigheter, men också andra aktörer.

Av *punkten 2* följer att Försvarets radioanstalt får behandla personuppgifterna med anledning av samarbete om utvecklingsverksamhet med andra länder eller internationella organisationer enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet.

Enligt *punkten 3* får Försvarets radioanstalt även behandla personuppgifterna om det är nödvändigt att tillhandahålla information som behövs i försvarsunderrättelseverksamheten för de ändamål som anges i 2 och 3 §§.

Genom *punkten 4* får behandling av personuppgifterna även ske i Försvarets radioanstalts informationssäkerhetsverksamhet för de ändamål som anges i 7 §.

Enligt *punkten 5* får Försvarets radioanstalt även vidarebehandla personuppgifterna om det är nödvändigt för att tillhandahålla information som behövs för att biträda andra myndigheter i den utsträckning det följer av lag eller förordning eller om regeringen har beslutat om det i ett enskilt fall.

Informationssäkerhetsverksamhet

7 § 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 beslut av regeringen i ett enskilt fall.

Paragrafen reglerar ändamålet för behandlingen av personuppgifter i Försvarets radioanstalts informationssäkerhetsverksamhet. Övervägandena finns i avsnitt 7.3.3.

Enligt *första meningen* får behandling av personuppgifter 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 radioanstalt får 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 (4 § förordningen [2007:937] med

instruktion för Försvarets radioanstalt och 17 § förordningen [2015:1053] om totalförsvar och höjd beredskap). Försvarets radioanstalts stöd innebär bl.a. att Försvarets radioanstalt på uppdragsgivarens begäran söker efter och analyserar brister i säkerheten i datorsystemen.

Av *andra meningen* framgår att uppgiften att lämna stöd till andra verksamheter ska följa av lag eller förordning eller ett beslut av regeringen i ett enskilt fall.

8 § Personuppgifter som behandlas med stöd av 7 § 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 har beslutat om det i ett enskilt fall,
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 5 §.

Paragrafen reglerar sekundära ändamål för behandling av personuppgifter som först kommit att behandlas inom informationssäkerhetsverksamheten. Övervägandena finns i avsnitt 7.3.3.

I *punkten 1* anges att Försvarets radioanstalt även får behandla personuppgifterna för att tillhandahålla information som behövs i verksamhet hos den som tar emot uppgifter om informationssäkerhet. Det kan röra sig om andra myndigheter och andra aktörer för vilkas räkning Försvarets radioanstalt har utfört aktiva it-kontroller eller installerat ett tekniskt detekterings- och varningssystem.

Av *punkten 2* följer att Försvarets radioanstalt får behandla personuppgifterna inom ramen för nationell och internationell samverkan på informationssäkerhetsområdet. Behandling får endast ske i den utsträckning det följer av lag eller förordning eller om regeringen har beslutat om det i ett enskilt fall.

Genom *punkten 3* får Försvarets radioanstalt även vidarebehandla personuppgifter om det är nödvändigt för att tillhandahålla information som behövs för vissa syften som anges i 1 § andra stycket lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet. Det ska vara fråga om att kartlägga allvarliga yttre hot mot samhällets infrastruktur (andra stycket 5) och främmande underrättelseverksamhet mot svenska intressen (andra stycket 7).

Genom *punkten 4* får vidarebehandling av personuppgifter även ske i Försvarets radioanstalts utvecklingsverksamhet för de ändamål som anges i 5 §.

Övriga ändamål

9 § Försvarets radioanstalt får behandla personuppgifter som utgör allmänt tillgänglig information om det är nödvändigt för den verksamhet som anges i 2, 5 och 7 §§.

Paragrafen ger stöd för behandling av personuppgifter som utgör allmänt tillgänglig information. Övervägandena finns i avsnitt 7.4.

Försvarets radioanstalt får enligt paragrafen behandla personuppgifter som utgör allmänt tillgänglig information om det är nödvändigt för den verksamhet som anges i 2, 5 och 7 §§. För att kunna bedriva en effektiv försvarsunderrättelseverksamhet behöver Försvarets radioanstalt, utöver den information som myndigheten inhämtar genom särskilda metoder, också ha god tillgång till allmänt tillgänglig information. Därigenom kan den på särskilt sätt inhämtade informationen på ett bättre sätt sättas in i sitt rätta sammanhang. Motsvarande behov finns i myndighetens utvecklingsverksamhet och informationssäkerhetsverksamhet. Av intresse här är framför allt information som utgörs av personuppgifter som kan påträffas vid sökning på internet eller vid sökningar i öppna databaser.

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

I paragrafen anges att Försvarets radioanstalt får behandla personuppgifter för vetenskapliga, statistiska eller historiska ändamål inom lagens tillämpningsområde. Övervägandena finns i avsnitt 7.5.

Genom paragrafen ges Försvarets radioanstalt möjlighet att behandla personuppgifter för vetenskapliga, statistiska eller historiska ändamål.

Författningsenlig och korrekt behandling

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

Paragrafen reglerar författningsenlig och korrekt behandling av personuppgifter. Övervägandena finns i avsnitt 8.1.1.

Enligt paragrafen ska personuppgifter behandlas författningsenligt och på ett korrekt sätt.

Att behandlingen ska ske författningsenligt innebär att den ska ske i enlighet med lag eller annan författning. Författningarna är även av betydelse för att en behandling ska anses ske på ett korrekt sätt. Vad som är ett korrekt sätt för behandling styrs dock inte enbart av författning. Tillsynsmyndighetens beslut om allmänna råd och uttalanden i fråga om personuppgiftsbehandling har också betydelse, liksom Försvarets radioanstalts interna regler.

Otillåten behandling av personuppgifter kan i vissa fall vara straffbar enligt bestämmelser i brottsbalken, bl.a. bestämmelsen i 4 kap. 9 c § brottsbalken om dataintrång. Tänkbara exempel på dataintrång kan vara externa angrepp eller att någon som har tillgång till ett it-system överskrider sina befogenheter.

Personuppgifternas kvalitet

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

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 reglerar personuppgifternas kvalitet. Övervägandena finns i avsnitt 8.1.2.

Enligt *första stycket* ska de behandlade uppgifterna vara riktiga och, om det är nödvändigt uppdaterade. Personuppgifterna ska också vara adekvata och relevanta i förhållande till ändamålet med behandlingen.

En personuppgift är riktig om den stämmer överens med de verkliga förhållandena. För att bestämma vilka de verkliga förhållandena är får man söka ledning i ändamålen med behandlingen. Det är ändamålen i det enskilda fallet som avses. Inom lagens tillämpningsområde måste frågan om en personuppgift är riktig inte bara vägas mot ändamålen med behandlingen utan även ses mot bakgrund av vad uppgiften rör, när den lämnas och vem som lämnar den. För att kunna avgöra om personuppgifterna är riktiga är det också av stor betydelse att veta om de grundar sig på fakta eller på personliga bedömningar. Kravet på att personuppgifter ska vara riktiga innebär inte något hinder mot att samla in exempelvis osäkra underrättelseuppgifter, under förutsättning att personuppgifterna är relevanta för arbetet och att det framgår att det är osäkert om uppgiften är riktig.

De personuppgifter som behandlas behöver vara uppdaterade bara om det är nödvändigt. Frågan om det är nödvändigt att de är uppdaterade får avgöras med hänsyn till ändamålen med behandlingen. Exempelvis kan uppgifter om telefonnummer eller andra kontaktuppgifter ändras under handläggningen av ett ärende och därmed behöva uppdateras.

Att personuppgifterna ska vara adekvata och relevanta innebär att ovidkommande uppgifter inte får behandlas. En prövning av om en personuppgift är nödvändig för behandlingen ska göras kontinuerligt av Försvarets radioanstalt, 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.

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. Uppgifter om utseende är inte i sig att betrakta som känsliga personuppgifter.

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 person-uppgifter är förutsättningarna för att behandla personuppgifterna inte uppfyllda.

Känsliga personuppgifter

13 § 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 personuppgifter behandlas får de dock kompletteras med sådana uppgifter som avses i första stycket, om det är absolut nödvändigt med hänsyn till ändamålen med behandlingen.

Paragrafen, som utformas enligt *Lagrådets* förslag, reglerar känsliga personuppgifter. Övervägandena finns i avsnitt 8.2.

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 typiskt sett inte en känslig personuppgift och den får alltså behandlas, med den begränsning som följer av 12 § 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 (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.

Andra stycket innehåller ett undantag från huvudregeln att känsliga personuppgifter inte får behandlas. Personuppgifter som behandlas på annan grund får kompletteras med känsliga personuppgifter, om det är absolut nödvändigt med hänsyn till ändamålen med behandlingen. Det innebär att personuppgifter som samlas in i ett visst fall får 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.

I 14 och 15 § finns ytterligare bestämmelser om behandling av känsliga personuppgifter.

14 § Biometriska uppgifter får behandlas om det är absolut nödvändigt med hänsyn till ändamålen med behandlingen.

Genetiska uppgifter får inte behandlas.

Paragrafen, som utformas enligt *Lagrådets* förslag, reglerar i vilken utsträckning biometriska uppgifter får behandlas. Övervägandena finns i avsnitt 8.2.

Enligt *första stycket* får biometriska uppgifter behandlas om det är absolut nödvändigt med hänsyn till ändamålen med behandlingen. Stycket möjliggör användning av särskild teknisk behandling för att bekräfta 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 varje enskilt fall.

I *andra stycket* anges att Försvarets radioanstalt inte får behandla genetiska uppgifter. Stycket innebär ett förbud för Försvarets radioanstalt att behandla sådana uppgifter.

15 § 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 med hänsyn till ändamålen med behandlingen. Detsamma gäller biometriska uppgifter.

Paragrafen, som utformas enligt *Lagrådets* förslag, reglerar i vilken utsträckning känsliga personuppgifter får användas som sökbegrepp. Övervägandena finns i avsnitt 8.2.

Paragrafen gäller generellt, dvs. för såväl personuppgifter som har gjorts gemensamt tillgängliga som personuppgifter som inte har det.

Paragrafen 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 med hänsyn till något av de ändamål för vilket Försvarets radioanstalt behandlar personuppgifter.

Försvarets radioanstalt kan behöva söka på uppgifter som rör politiska åsikter, religiös övertygelse eller etniskt ursprung, eftersom det ingår i Försvarets radioanstalts uppdrag att kartlägga sådan verksamhet som kan komma att hota Sveriges försvar och säkerhet.

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 13 §. Rätten att göra en sökning medför således inte en generell rätt att fortsätta att behandla uppgifterna.

Personnummer och samordningsnummer

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

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

Paragrafen reglerar i vilken omfattning personnummer eller samordningsnummer får behandlas vid Försvarets radioanstalt. Övervägandena finns i avsnitt 8.3.

Enligt paragrafen får uppgifter om personnummer eller samordningsnummer bara behandlas när det är klart motiverat med hänsyn till ändamålen med behandlingen (*punkten 1*), vikten av en säker identifiering (*punkten 2*), eller något annat beaktansvärt skäl (*punkten 3*).

Vad som avses med personnummer och samordningsnummer framgår av folkbokföringslagen (1991:1487). Bestämmelsen innebär att en

intresseavvägning mellan behovet av behandlingen och de integritetsrisker som den innebär ska göras. Om behandlingen av personnummer eller samordningsnummer inte är klart motiverad med hänsyn till dess ändamål, till vikten av en säker identifiering eller något annat beaktansvärt skäl får den inte utföras.

Om den registrerade har offentliggjort personuppgifterna

17 § Trots 13, 14 och 16 §§ får andra personuppgifter än genetiska uppgifter behandlas, om den registrerade på ett tydligt sätt har offentliggjort uppgifterna.

Paragrafen reglerar behandling av vissa personuppgifter om den registrerade har offentliggjort uppgifterna. Övervägandena finns i avsnitt 8.4.

Paragrafen ger Försvarets radioanstalt möjlighet att, med undantag för genetiska uppgifter, behandla känsliga personuppgifter samt personnummer och samordningsnummer, om den registrerade på ett tydligt sätt har offentliggjort uppgifterna. Så kan exempelvis vara fallet om den registrerade har gjort personuppgifterna tillgängliga på internet.

Behandling av personuppgifter i vissa fall

18 § Hantering av information som innebär behandling av personuppgifter ska inte anses oförenlig med bestämmelserna i 1, 2, 5, 7, 9, 11–14 och 16 §§ i det skede av behandlingen då det inte har kunnat fastställas vilka personuppgifter som informationen innehåller.

Paragrafen reglerar behandling av personuppgifter i vissa fall. Övervägandena finns i avsnitt 8.5.

Försvarets radioanstalt kan såväl i myndighetens signalspaning i försvarsunderrättelseverksamhet som i dess informationssäkerhetsverksamhet komma att hantera information som är krypterad och formulerad på ett främmande språk. Innan dess att informationen har bearbetats finns inte förutsättningar för att bedöma om den innehåller personuppgifter. Den initiala behandling som krävs för att detta ska kunna klarläggas måste kunna äga rum utan hinder av bestämmelserna om ändamål, författningsenlig och korrekt behandling, personuppgifternas kvalitet, känsliga personuppgifter samt personnummer och samordningsnummer. Genom paragrafen tydliggörs att hantering av information som innebär behandling av personuppgifter inte ska anses oförenlig med bestämmelserna i 1, 2, 5, 7, 9, 11–14 och 16 §§ 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 Försvarets radioanstalt behandla dem enligt bestämmelserna i lagen.

Längsta tid som personuppgifter får behandlas

19 § Personuppgifter får inte behandlas under längre tid än vad som behövs med hänsyn till ändamålen med behandlingen.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om att personuppgifter får

behandlas under endast viss tid eller fortsätta behandlas för arkivändamål av allmänt intresse eller för vetenskapliga, statistiska eller historiska ändamål.

Regeringen eller den myndighet som regeringen bestämmer får också besluta om sådan behandling i ett enskilt fall.

Paragrafen reglerar längsta tid som personuppgifter får behandlas. Övervägandena finns i avsnitt 8.6.

Enligt *första stycket* får personuppgifter inte behandlas under längre tid än vad som behövs med hänsyn till ändamålen med behandlingen. Att det inte längre finns behov av att behandla personuppgiften enligt ett visst ändamål medför inte att behandlingen av den måste upphöra för alla ändamål samtidigt. Det förhållandet att personuppgiften fortfarande behövs för ett visst ändamål innebär dock inte att uppgiften får fortsätta att behandlas för alla ändamål lika länge. 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.

Stycket ger även stöd för fortsatt behandling av personuppgifter i ett avslutat ärende om uppgifterna bedöms ha ett allmänt värde för exempelvis Försvarets radioanstalts försvarsunderrättelseverksamhet eller informationssäkerhetsverksamhet. En grundläggande förutsättning för fortsatt behandling är att Försvarets radioanstalt bedömer att uppgifterna behöver finnas tillgängliga ytterligare en viss tid för något av de ändamål för vilka myndigheten 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.

Stycket hindrar inte att Försvarets radioanstalt med stöd i annan författning arkiverar och bevarar allmänna handlingar eller att arkivmaterial lämnas till en arkivmyndighet.

I *andra stycket* finns en upplysningsbestämmelse om att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter om att personuppgifter får behandlas under endast viss tid eller fortsätta behandlas för arkivändamål av allmänt intresse eller för vetenskapliga, statistiska eller historiska ändamål.

Enligt *tredje stycket* får regeringen eller den myndighet som regeringen bestämmer också besluta om sådan behandling i ett enskilt fall.

Överföring av personuppgifter till en mottagare utomlands

20 § Personuppgifter som behandlas med stöd av denna lag får föras över till ett annat land eller en internationell organisation endast om det är nödvändigt för att Försvarets radioanstalt ska kunna fullgöra sina uppgifter inom ramen för det internationella försvarsunderrättelse- och säkerhetssamarbetet och

1. överföringen riktas till en utländsk underrättelse- eller säkerhetstjänst, eller ett underrättelse- eller säkerhetsorgan i en internationell organisation,
2. sekretess inte hindrar en överföring, och
3. mottagaren garanterar tillräckligt skydd för personuppgifterna.

Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om att överföring får ske även i andra fall än som anges i första stycket 1.

Regeringen får också besluta om sådan överföring i ett enskilt fall.

Paragrafen reglerar överföring av personuppgifter till en mottagare utomlands. Övervägandena finns i avsnitt 10.5. Rubriken närmast före paragrafen utformas enligt *Lagrådets* förslag.

Av *första stycket* framgår att överföring av personuppgifter som behandlas med stöd av lagen får ske endast om det är nödvändigt för att Försvarets radioanstalt ska kunna fullgöra sina uppgifter inom ramen för det internationella försvarsunderrättelse- och säkerhetssamarbetet. Vidare anges ett antal villkor som ska vara uppfyllda för att Försvarets radioanstalt ska få överföra personuppgifter till ett annat land eller en internationell organisation. *Första stycket 1–3* är kumulativa, dvs. samtliga villkor enligt punkterna måste vara uppfyllda för att en överföring av personuppgifter ska vara tillåten.

Genom *första stycket 1* avgränsas de utländska mottagare till vilka personuppgifter får överföras. Personuppgifter får endast överföras till en underrättelse- eller säkerhetstjänst i ett annat land eller till ett underrättelse- eller säkerhetsorgan i en internationell organisation. EU, FN och Nato är exempel på internationella organisationer som har denna typ av organ.

Överföring av personuppgifter får endast ske om sekretess inte hindrar det. Detta anges i *första stycket 2*. En sekretessprövning behöver således alltid utföras som en del i bedömningen om en överföring av personuppgifter ska ske.

Första stycket 3 ställer krav på att en viss skyddsnivå ska föreligga för att personuppgifter ska kunna överföras till ett annat land eller en internationell organisation. Om personuppgifter ska överföras till en internationell organisation är det organisationen som sådan, inte de enskilda stater som är medlemmar i organisationen, som ska uppfylla kravet på skyddsnivå. Försvarets radioanstalt ska bedöma alla omständigheter kring överföringen och komma till slutsatsen att skyddsåtgärderna är tillräckliga. Om en mottagande stat är ansluten till dataskyddskonventionen eller en annan internationell överenskommelse som innehåller bestämmelser om dataskydd och registrerades rättigheter kan lämpliga skyddsåtgärder som utgångspunkt anses föreligga. Att den som ska behandla personuppgifterna i det andra landet eller i den internationella organisationen kommer att ha tystnadsplikt som omfattar de överförda uppgifterna eller att det garanteras att personuppgifterna inte kommer att behandlas för något annat ändamål än det för vilket de överförs kan också beaktas. Detsamma gäller i fråga om åtaganden från mottagarens sida om att inte föra personuppgifterna vidare eller att inte använda personuppgifterna efter en viss tidpunkt, eller att förstöra dem

I *andra stycket* finns en upplysningsbestämmelse om att regeringen kan meddela föreskrifter om att överföring även får ske i andra fall än som anges i första stycket 1 och enligt *tredje stycket* får regeringen också besluta om sådan överföring i ett enskilt fall. Det kan t.ex. vid internationella militära insatser vara nödvändigt att överlämna underrättelser till en funktion i en annan stat som inte kan sägas vara en underrättelse- eller säkerhetstjänst.

Utlämnande av personuppgifter

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

Paragrafen reglerar utlämnande av personuppgifter. Övervägandena finns i avsnitt 10.2.

I paragrafen anges att personuppgifter får lämnas ut elektroniskt på annat sätt än genom direktåtkomst om regeringen har meddelat föreskrifter eller beslutat om det i ett enskilt fall.

3 kap. Gemensamt tillgängliga personuppgifter

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. Med att göra personuppgifter gemensamt tillgängliga avses inte att endast ett fåtal personer får tillgång till uppgifterna.

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

Regeringen eller den myndighet som regeringen bestämmer får också besluta om uppgiftssamlingar i ett enskilt fall.

Paragrafen reglerar personuppgifter som får göras gemensamt tillgängliga. Övervägandena finns i avsnitt 9.

I *första stycket* anges genom en hänvisning till i lagen angivna ändamål vilka personuppgifter som får göras gemensamt tillgängliga. Vidare anges att med att göra personuppgifter gemensamt tillgängliga avses inte att endast ett fåtal personer får tillgång till uppgifterna. 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.

I *andra stycket* finns en upplysningsbestämmelse om att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter om vilka uppgiftssamlingar som får finnas och vilka uppgifter som får behandlas i respektive uppgiftssamling.

Enligt *tredje stycket* får regeringen eller den myndighet som regeringen bestämmer också får besluta om uppgiftssamlingar i ett enskilt fall.

Direktåtkomst

Försvarsunderrättelseverksamhet

2 § Säkerhetspolisen och Försvarsmakten får medges direktåtkomst till personuppgifter som utgör analysresultat inom försvarsunderrättelseverksamheten och som finns i uppgiftssamlingar.

Säkerhetspolisen och Försvarsmakten har rätt att vid direktåtkomst ta del av de personuppgifter som omfattas av åtkomsten.

Paragrafen reglerar Säkerhetspolisens och Försvarsmaktens direktåtkomst till vissa uppgifter som Försvarets radioanstalt behandlar. Övervägandena finns i avsnitt 10.3.1.

I *första stycket* anges att Säkerhetspolisen och Försvarsmakten får medges direktåtkomst till personuppgifter som utgör analysresultat inom försvarsunderrättelseverksamheten och som finns i uppgiftssamlingar. Analysresultat består av information som ännu inte har bearbetats till underrättelserapporter.

Andra stycket innehåller en sekretessbrytande bestämmelse som möjliggör för Säkerhetspolisen och Försvarsmakten att vid direktåtkomst få ta del av uppgifter som omfattas av sekretess.

3 § Om det behövs för samarbetet mot terrorism eller för annat internationellt säkerhetssamarbete, får en utländsk underrättelse- eller säkerhetstjänst medges direktåtkomst till personuppgifter som behandlas med stöd av 2 kap. 2 § och som finns i uppgiftssamlingar.

Första stycket gäller enbart i den utsträckning som sådan direktåtkomst följer av lag eller förordning eller om regeringen har beslutat om den i ett enskilt fall.

I paragrafen regleras Försvarets radioanstalts möjlighet att medge en utländsk underrättelse- och säkerhetstjänst direktåtkomst till vissa personuppgifter. Övervägandena finns i avsnitt 10.3.2.

Av *första stycket* framgår att en utländsk underrättelse- eller säkerhetstjänst får medges direktåtkomst till personuppgifter som behandlas med stöd av 2 kap. 2 § och som finns i uppgiftssamlingar, om det behövs för samarbetet mot terrorism eller vid svenskt deltagande i annat internationellt underrättelse- och säkerhetssamarbete. Möjligheten att dela information genom direktåtkomst begränsas till utländska underrättelse- och säkerhetstjänster. Direktåtkomst får endast medges till personuppgifter som behandlas i Försvarets radioanstalts försvarsunderrättelseverksamhet och som finns i uppgiftssamlingar.

Innan direktåtkomst medges måste Försvarets radioanstalt avgöra om det finns sakliga skäl att låta en viss utländsk underrättelse- eller säkerhetstjänst få ta del av personuppgifterna, dvs. om det finns behov av att lämna ut uppgifterna för att främja bekämpningen av terrorism eller andra svenska intressen. Innan personuppgifterna lämnas ut genom direktåtkomst ska Försvarets radioanstalt dessutom bedöma om det finns rättsliga förutsättningar att lämna ut dem till en utländsk mottagare, bl.a. med beaktande av sekretess.

Enligt *andra stycket* gäller första stycket endast i den utsträckning som sådan direktåtkomst följer av lag eller förordning eller om regeringen har beslutat om den i ett enskilt fall.

Informationssäkerhetsverksamhet

4 § Om det behövs för samarbetet mot it-relaterade hot mot samhällsviktiga system, får en utländsk organisation inom informationssäkerhetsområdet medges direktåtkomst till personuppgifter som behandlas med stöd av 2 kap. 7 § och som finns i uppgiftssamlingar.

Första stycket gäller enbart i den utsträckning som sådan direktåtkomst följer av lag eller förordning eller om regeringen har beslutat om den i ett enskilt fall.

Paragrafen anger när Försvarets radioanstalt får medge en utländsk organisation inom informationssäkerhetsområdet direktåtkomst. Övervägandena finns i avsnitt 10.3.2.

I *första stycket* anges att direktåtkomst får medges en utländsk organisation inom informationssäkerhetsområdet vid samarbetet mot it-relaterade hot mot samhällsviktiga system om det är nödvändigt för samarbetet. Direktåtkomst får endast avse personuppgifter som behandlas inom Försvarets radioanstalts informationssäkerhetsverksamhet och som finns i uppgiftssamlingar.

I *andra stycket* tydliggörs att direktåtkomst enligt första stycket endast gäller i den utsträckning som sådan åtkomst följer av lag eller förordning eller om regeringen har beslutat om den i ett enskilt fall.

Direktåtkomst i andra fall

5 § Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om direktåtkomst till uppgiftssamlingar i andra fall än de som anges i 2–4 §§.

Regeringen får också besluta om detta i ett enskilt fall.

Paragrafen reglerar direktåtkomst i andra fall. Övervägandena finns i avsnitten 10.3.1 och 10.3.2.

Första stycket innehåller en upplysningsbestämmelse om att regeringen kan meddela föreskrifter om att andra än de som anges i 2–4 §§ får ha direktåtkomst till uppgiftssamlingar.

Enligt *andra stycket* får regeringen också besluta om detta i ett enskilt fall.

Enligt regeringsformen får skyddet gentemot det allmänna mot vissa fall av betydande intrång i den personliga integriteten begränsas enbart genom lag (2 kap. 6 § andra stycket och 20–21 §§ regeringsformen). Regeringens möjlighet att meddela föreskrifter är således begränsad.

Omfattningen av direktåtkomsten

6 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om omfattningen av direktåtkomsten och om behörighet och säkerhet vid sådan åtkomst.

Regeringen får också besluta om detta i ett enskilt fall.

Paragrafen reglerar omfattningen av direktåtkomsten. Övervägandena finns i avsnitten 10.3.1 och 10.3.2.

Första stycket innehåller en upplysningsbestämmelse om att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter om omfattningen av direktåtkomsten, och om behörighet och säkerhet vid sådan åtkomst.

Enligt *andra stycket* får regeringen också besluta om detta i ett enskilt fall.

4 kap. Skyldigheter 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 att de registrerades rättigheter skyddas.

Paragrafen reglerar åtgärder för att säkerställa författningsenlig behandling. Övervägandena finns i avsnitt 11.3.1.

Tekniska och organisatoriska åtgärder för att skydda personuppgifterna regleras i 3 §.

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. Åtgärder som vidtas för att visa att behandlingen är författningsenligt kan t.ex. vara dokumentation av it-system, behandlingar och vidtagna åtgärder samt teknisk spårbarhet genom loggning och logguppföljning. 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 § Tillgången till personuppgifter ska begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter.

Paragrafen reglerar den interna tillgången till personuppgifter för dem som arbetar vid Försvarets radioanstalt. Övervägandena finns i avsnitt 11.3.2.

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 Försvarets radioanstalt 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 Försvarets radioanstalts 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.

Paragrafen gäller enligt 10 § även för personuppgiftsbiträden som Försvarets radioanstalt anlitar.

Säkerheten för personuppgifter

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

I paragrafen regleras säkerheten för personuppgifter. Övervägandena finns i avsnitt 11.3.2.

Enligt paragrafen ska Försvarets radioanstalt 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, som illustrerar vad skyddsåtgärderna ska åstadkomma, 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.

Tänkbara exempel på organisatoriska skyddsåtgärder kan vara 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 Försvarets radioanstalt i det enskilda fallet. Bedömningen är bl.a. beroende av vilka personuppgifter som behandlas och hur integritetskänsliga de är.

Paragrafen gäller enligt 10 § även för personuppgiftsbiträden som Försvarets radioanstalt anlitar.

Dataskyddsombud

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

Paragrafen reglerar skyldighet att utse dataskyddsombud. Övervägandena finns i avsnitt 11.4.

Enligt paragrafen ska ett eller flera dataskyddsombud utses. Dataskyddsombudet ska vara anställt hos Försvarets radioanstalt. Försvarets radioanstalt ska anmäla till tillsynsmyndigheten när dataskyddsombud utses och entledigas.

5 § Ett dataskyddsombud 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. vara kontaktpunkt för enskilda i frågor som rör Försvarets radioanstalts behandling av personuppgifter, och

4. vid behov söka vägledning av tillsynsmyndigheten.

I paragrafen anges vilka uppgifter ett dataskyddsombud ska utföra. Övervägandena finns i avsnitt 11.4.

Enligt *punkten 1* ska ett dataskyddsombud självständigt 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.

Dataskyddsombudet bör framför allt granska den praktiska hanteringen av personuppgifter. Därutöver bör ombudet 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 ett 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. Ombudet förutsätts också ha goda kunskaper om regelverket om personuppgiftsbehandling.

I *punkten 2* anges att ett dataskyddsombud ska informera och ge råd till Försvarets radioanstalt och till dem som behandlar personuppgifter under myndighetens ledning om deras skyldigheter vid sådan behandling. Det handlar främst om att göra den Försvarets radioanstalt 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 dataskyddsombudet ska tala om för Försvarets radioanstalt och medarbetarna hur de ska behandla personuppgifter i enskilda fall.

Ett dataskyddsombud ska vara kontaktpunkt för enskilda i frågor som rör behandling av personuppgifter, vilket anges i *punkten 3*.

Enligt *punkten 4* ska ett dataskyddsombud vid behov söka vägledning av tillsynsmyndigheten. Det innebär att ombudet vid tveksamheter av olika slag bör fråga tillsynsmyndigheten om råd.

Ett dataskyddsombud behöver inte uteslutande utföra enbart de arbetsuppgifter som anges i paragrafen. Arbetet som dataskyddsombud kan kombineras med andra arbetsuppgifter, så länge de inte kommer i konflikt med uppdraget som dataskyddsombud.

Personuppgiftsbiträden

6 § 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 registrerades rättigheter.

Paragrafen reglerar anlitande av personuppgiftsbiträden. Övervägandena finns i avsnitt 11.5.2.

Försvarets radioanstalt 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. Enligt paragrafen ska Försvarets radioanstalt 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.

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

Paragrafen reglerar förhållandet mellan Försvarets radioanstalt och personuppgiftsbiträden. Övervägandena finns i avsnitt 11.5.2.

Av paragrafen följer att det ska finnas ett skriftligt avtal eller en annan skriftlig överenskommelse med personuppgiftsbiträden som reglerar personuppgiftsbiträdets behandling av personuppgifter för Försvarets radioanstalts räkning. Eftersom statliga myndigheter ingår i samma juridiska person – staten, i rättslig mening inte kan ingå bindande avtal med varandra får de ingå en skriftlig överenskommelse som reglerar behandlingen om en myndighet agerar personuppgiftsbiträde åt en annan.

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

Paragrafen reglerar möjligheten för ett personuppgiftsbiträde att anlita ett annat personuppgiftsbiträde. Övervägandena finns i avsnitt 11.5.2.

Enligt paragrafen får ett personuppgiftsbiträde inte anlita ett annat personuppgiftsbiträde, ett s.k. underbiträde, utan skriftligt tillstånd från Försvarets radioanstalt. Ett sådant tillstånd kan gälla personuppgiftsbiträdets rätt att anlita underbiträden generellt eller i en specifik situation. Syftet med paragrafen är att Försvarets radioanstalt ska känna till vilka personuppgiftsbiträden som behandlar personuppgifter för myndighetens räkning.

9 § 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.

Paragrafen reglerar behandling av personuppgifter hos ett personuppgiftsbiträde. Övervägandena finns i avsnitt 11.5.3.

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 att skydda personuppgifterna. Om det finns avvikande bestämmelser i annan lagstiftning som anger att personuppgiftsbiträdet är skyldigt 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.

10 § Försvarets radioanstalts skyldigheter enligt 2 och 3 §§ gäller även för personuppgiftsbiträden som Försvarets radioanstalt anlitar.

Paragrafen kopplar Försvarets radioanstalts skyldigheter i egenskap av personuppgiftsansvarig till att gälla även för personuppgiftsbiträden. Övervägandena finns i avsnitt 11.5.4.

Att personuppgiftsbiträden åläggs vissa skyldigheter fråntar inte Försvarets radioanstalt dess ansvar som personuppgiftsansvarig. 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 Försvarets radioanstalt.

Vad som närmare gäller för ett personuppgiftsbiträde framgår av författningskommentaren till 2 och 3 §§.

5 kap. Enskildas rättigheter

Rätten till information

Allmän information

1 § Försvarets radioanstalt ska göra följande information allmänt tillgänglig:

1. myndighetens identitet och kontaktuppgifter,
2. uppgifter om dataskyddsombudet,
3. kategorier av ändamålen med behandlingen av personuppgifter,
4. rätten enligt 2 § att begära att få information om behandlingen av personuppgifter och att få del av dem, och
5. rätten att begära rättelse, radering eller begränsning av behandlingen enligt 5 §.

Paragrafen reglerar krav på att göra viss information allmänt tillgänglig. Övervägandena finns i avsnitt 12.1.1.

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.

Försvarets radioanstalt är enligt 4 kap. 4 § skyldig att utse ett eller flera 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.

Kategorier av ändamål för behandlingen av personuppgifter ska framgå, vilket anges i *punkten 3*. Det är inte ändamålen med behandlingen av personuppgifter i enskilda fall som avses utan för vilka kategorier av ändamål som myndigheten behandlar personuppgifter. Kategorier av ändamål kan t.ex. vara underrättelsearbete, utvecklingsarbete och informationssäkerhetsarbete.

Enligt *punkterna 4* och *5* ska Försvarets radioanstalt upplysa om de rättigheter som enskilda har enligt 2 och 5 §§. 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 efter begäran

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

1. vilka personuppgifter om den sökande som behandlas,
2. varifrån personuppgifterna kommer,
3. ändamålen med behandlingen,
4. mottagare eller kategorier av mottagare av personuppgifterna, även i annat land eller internationella organisationer,
5. hur länge personuppgifterna får behandlas eller, om det inte är möjligt att ange, kriterierna för att fastställa det, och
6. rätten att begära rättelse, radering eller begränsning av behandlingen enligt 5 §.

Ett utlämnande av personuppgifter enligt första stycket behöver inte omfatta sådana 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 om information enligt första stycket ska göras skriftligen hos Försvarets radioanstalt och vara undertecknad av den sökande själv. Informationen 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 information som ska lämnas efter begäran. Övervägandena finns i avsnitt 12.1.2.

I *första stycket 1–6* anges vilken skriftlig information sökanden kan få del av.

Enligt *första stycket 1* ska i den skriftliga informationen anges vilka personuppgifter om den sökande som behandlas.

Enligt *första stycket 2* ska anges varifrån personuppgifterna kommer.

Enligt *första stycket 3* ska ändamålen med behandlingen anges.

Enligt *första stycket 4* ska mottagare eller kategorier av mottagare av personuppgifterna, även i annat land eller internationella organisationer, anges.

Enligt *första stycket 5* ska det anges hur länge personuppgifterna får behandlas eller, om det inte är möjligt att ange, kriterierna för att fastställa det.

Enligt *första stycket 6* ska rätten att begära rättelse, radering eller begränsning av behandlingen enligt 5 § anges.

Av *andra stycket* följer att sådana personuppgifter som sökanden har tagit del av som utgångspunkt inte omfattas av skyldigheten att lämna ut uppgifterna. Sökanden ska dock informeras om att personuppgifterna i fråga behandlas.

Av *tredje stycket* framgår kraven på en begäran om information.

Begränsning av rätten till information

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

Om det gäller sekretess är Försvarets radioanstalt inte skyldig att redovisa skälen för ett beslut enligt första stycket eller ett beslut i fråga om rättelse, radering eller begränsning av behandlingen enligt 5 §.

I paragrafen regleras begränsningar av rätten till information. Övervägandena finns i avsnitt 12.2.

Många uppgifter som behandlas i Försvarets radioanstalts 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 registrerade.

Enligt *andra stycket* är Försvarets radioanstalt inte heller skyldig att redovisa skälen för ett beslut enligt första stycket eller ett 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.

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

Informationsskyldigheten gäller dock om uppgifterna

1. har lämnats ut till tredje part, med undantag för en myndighet som med stöd av författning utövar tillsyn, kontroll eller revision,
2. behandlas enbart för statistiska ändamål eller arkivändamål av allmänt intresse, eller
3. har behandlats under längre tid än ett år i löpande text som inte har fått sin slutliga utformning.

I paragrafen regleras vissa undantag från informationsskyldigheten för personuppgifter i viss typ av text. Övervägandena finns i avsnitt 12.2.

Den personuppgiftsansvariges skyldighet att lämna personrelaterad information enligt 2 § gäller enligt *första stycket* inte för personuppgifter i löpande text som inte fått sin slutliga utformning när begäran gjordes eller text som utgör en minnesanteckning 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 tillför ärendet något i sak.

Av *andra stycket* framgår att undantaget från informationsskyldigheten enligt första stycket 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. Enligt *andra stycket 1* gäller undantaget inte om personuppgifterna har lämnats ut till tredje part, såvida det inte är fråga om en myndighet som med stöd av författning utövar tillsyn, kontroll eller revision. Det är den version av uppgifterna i t.ex. utkastet som lämnades till tredje part som informationsskyldigheten omfattar, även om utkastet därefter har ändrats.

Undantaget från informationsskyldigheten gäller enligt *andra stycket 2* inte heller om personuppgifterna behandlas enbart för statistiska ändamål eller arkivändamål av allmänt intresse. Om ett ärende har avslutats och utkastet eller minnesanteckningen har arkiverats eller om handlingarna endast används vid statistikproduktion ska alltså information om behandlingen av personuppgifterna lämnas ut. Avslutningsvis gäller undantaget inte heller för löpande text som inte fått sin slutliga utformning, om personuppgifterna har behandlats under längre tid än ett år, vilket framgår av *andra stycket 3*.

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 statistiska ändamål eller arkivändamål av allmänt intresse ska bedömas i förhållande till när begäran om information gjordes.

Rätten till rättelse, radering och begränsning av behandlingen

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

Om uppgifterna har lämnats ut till tredje part ska denne underrättas om en åtgärd enligt första stycket, om den registrerade begär det eller om en mera betydande skada eller olägenhet för den registrerade 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.

I paragrafen, som utformas med beaktande av *Lagrådets* synpunkter i fråga om andra stycket, regleras rätten till rättelse, radering eller begränsning av behandlingen av personuppgifter. Övervägandena finns i avsnitt 12.3.

Försvarets radioanstalt ska enligt *första stycket* på begäran av den registrerade snarast rätta, radera eller begränsa behandlingen av sådana personuppgifter som inte har behandlats i enlighet med denna lag eller

föreskrifter som har meddelats med stöd av lagen. Begäran kan framställas formlöst.

Kravet på att en åtgärd i form av rättelse, radering eller begränsning ska vidtas snarast innebär att Försvarets radioanstalt skyndsamt ska utreda frågan och, om det finns skäl för det, så fort som möjligt genomföra åtgärden.

Begränsning av behandlingen av personuppgifter kan komma i fråga om den registrerade bestrider att personuppgifterna är riktiga, men det inte är möjligt att fastställa om så är fallet. En felaktig personuppgift ska rättas snarast möjligt. Om Försvarets radioanstalts utredning om den omstridda personuppgiften inte kan slutföras tillräckligt snabbt kan behandlingen behöva begränsas under utredningstiden. Har behandlingen av en personuppgift begränsats får uppgiften som utgångspunkt inte längre behandlas av Försvarets radioanstalt, utom för de ändamål för vilka behandlingen begränsades. Uppgiften får dock lämnas ut med stöd av 2 kap. tryckfrihetsförordningen.

Försvarets radioanstalt ska vidta åtgärder som visar att behandlingen av en viss personuppgift har begränsats. En sådan åtgärd kan vara att föra över uppgiften från det datasystem där den behandlas, t.ex. myndighetens verksamhetssystem, till ett arkivsystem. Andra åtgärder kan vara att göra personuppgiften oåtkomlig genom en teknisk begränsning eller annan inskränkning av tillgången till uppgiften. När utredningen om personuppgiften är avslutad ska begränsningen av behandlingen upphöra. Då ska personuppgiften antingen rättas eller fortsätta att behandlas som tidigare.

Försvarets radioanstalt ska enligt *andra stycket* underrätta tredje part om en korrigering, om den registrerade 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 part redan har korrigerat uppgiften.

Enligt *tredje stycket* behöver någon underrättelse inte 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.

Avgiftsfri information

6 § Information enligt 1 § och information och uppgifter enligt 2 § ska lämnas utan avgift.

Paragrafen reglerar avgiftsfri information. Övervägandena finns i avsnitten 12.1.1 och 12.1.2.

Enligt paragrafen ska information enligt 1 § och information och uppgifter enligt 2 § lämnas utan avgift.

Tillsyn över personuppgiftsbehandlingen

1 § Den myndighet som regeringen bestämmer utövar tillsyn över Försvarets radioanstalts behandling av personuppgifter enligt denna lag, enligt föreskrifter som har meddelats i anslutning till lagen och enligt beslut med stöd av lagen.

Tillsynsmyndigheten ska, när det är motiverat, ge råd och stöd till Försvarets radioanstalt och personuppgiftsbiträden i frågor som gäller deras skyldigheter enligt lag eller annan författning.

I paragrafen, som utformas i linje med *Lagrådets* förslag, regleras tillsyn över personuppgiftsbehandlingen. Övervägandena finns i avsnitt 13.2.

Enligt *första stycket* ska tillsynsmyndigheten utöva tillsyn över Försvarets radioanstalts behandling av personuppgifter enligt lagen, enligt föreskrifter som har meddelats i anslutning till lagen och enligt beslut med stöd av lagen. 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 utomstående 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 lagen och i föreskrifter som har meddelats i anslutning till lagen.

Enligt *andra stycket* ska tillsynsmyndigheten, när det är motiverat, ge råd och stöd till Försvarets radioanstalt och personuppgiftsbiträden i frågor som gäller deras skyldigheter enligt lag eller annan författning. 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 motiverat. Rådgivningen och stödet ska avse Försvarets radioanstalts och personuppgiftsbiträdens skyldigheter. Stycket innebär således inte någon rätt för Försvarets radioanstalt eller personuppgiftsbiträden att avkräva tillsynsmyndigheten råd i en konkret fråga.

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 innehåller en upplysningsbestämmelse om att det i lagen om signalspaning i försvarsunderrättelseverksamhet finns särskilda bestämmelser om kontroll. Enligt 10 § i den lagen ska kontrollen särskilt avse granskning av sökbegrepp, förstöring av uppgifter samt rapportering.

Tillsynsmyndighetens befogenheter

Undersökningsbefogenheter

3 § Tillsynsmyndigheten har rätt att av Försvarets radioanstalt eller av 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. den hjälp och annan information som behövs för tillsynen.

I paragrafen regleras tillsynsmyndighetens undersökningsbefogenheter. Övervägandena finns i avsnitt 13.3.1.

Enligt *punkten 1* har tillsynsmyndigheten rätt att för sin tillsyn från Försvarets radioanstalt och ett personuppgiftsbiträde få tillgång till personuppgifter som behandlas. Det innebär att Försvarets radioanstalt eller personuppgiftsbiträdet ska lämna de begärda uppgifterna även om det kräver viss efterforskning.

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 som Försvarets radioanstalt 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 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 Försvarets radioanstalt 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. Punkten 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

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 motverka den risken.

Tillsynsmyndigheten får besluta om en skriftlig varning, om en planerad behandling av personuppgifter riskerar att strida mot lag eller annan författning.

Detsamma gäller om en pågående behandling riskerar att strida mot lag eller annan författning.

Paragrafen reglerar tillsynsmyndighetens befogenheter i det förebyggande arbetet. Övervägandena finns i avsnitt 13.3.2.

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 Försvarets radioanstalt eller personuppgiftsbiträdet att motverka risken genom råd, rekommendationer och påpekanden. Rådgivning kan avse såväl formella som informella samråd. De befogenheter som anges i stycket får även i vissa fall användas i korrigerande syfte, vilket framgår av 5 § första stycket 1.

Enligt *andra stycket* får tillsynsmyndigheten besluta om en skriftlig varning om en planerad behandling riskerar att stå i strid med lag eller annan författning. 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 beslutar om en varning. Av beslutet om varning ska framgå varför tillsynsmyndigheten bedömt att behandlingen inte kommer att vara författningsenlig. Ett beslut om varning har inte några rättsverkningar, men den som får en varning förväntas rätta sig efter den.

Varning får också beslutas om en pågående behandling riskerar att strida mot 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 på annat sätt 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 för att fullgöra andra skyldigheter, eller
2. besluta att förelägga Försvarets radioanstalt eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsenlig eller för att fullgöra andra skyldigheter.

Av ett beslut om föreläggande ska det framgå när föreläggandet senast ska ha följts och, om det är lämpligt, vilka åtgärder som ska vidtas.

I paragrafen, som utformas enligt förslag och efter synpunkter från *Lagrådet,* regleras tillsynsmyndighetens korrigerande befogenheter. Övervägandena finns i avsnitt 13.3.3.

Tillsynsmyndigheten har möjlighet att successivt använda olika medel och på så sätt öka påtryckningarna på den som inte självmant rättar sig.

De korrigerande befogenheterna får användas om tillsynsmyndigheten konstaterar att Försvarets radioanstalt 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. Försvarets radioanstalt 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 1* får tillsynsmyndigheten använda de förebyggande befogenheter som regleras i 4 § första stycket för att försöka förmå Försvarets radioanstalt eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsenlig eller för att fullgöra andra skyldigheter.

Enligt *första stycket 2* får tillsynsmyndigheten besluta att förelägga Försvarets radioanstalt eller personuppgiftsbiträdet att vidta åtgärder för att viss behandling av personuppgifter ska bli författningsenlig eller för att de ska uppfylla andra skyldigheter.

Av *andra stycket* framgår att det av ett beslut om föreläggande alltid ska framgå när föreläggandet senast ska ha följts ha följts 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 Försvarets radioanstalt 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 registrerade för den skada och kränkning av den personliga integriteten som orsakats av behandling av personuppgifter i strid med denna lag, föreskrifter som har meddelats i anslutning till lagen eller beslut med stöd av lagen.

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

I paragrafen regleras skadestånd. Övervägandena finns i avsnitt 14.3.2.

Av *första stycket* framgår att rätt till skadestånd kan uppkomma på grund av behandling i strid med bestämmelser i lagen, föreskrifter som har meddelats i anslutning till lagen eller beslut med stöd av lagen. För att den personuppgiftsansvarige ska bli ersättningsskyldig måste den registrerade bevisa att behandling av dennes personuppgifter stått i strid med bestämmelserna 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. Den praxis som finns om tillämpningen av bestämmelserna i den upphävda lagen (2007:259) om Försvarets radioanstalts behandling av personuppgifter i försvarsunderrättelse- och

utvecklingsverksamhet och personuppgiftslagen är avsedd att vara vägledande.

Av *andra stycket* följer att ersättningsskyldigheten, i den utsträckning det är skäligt, kan jämkas om den personuppgiftsansvarige visar att felet inte berodde på denne.

Överklagande

Överklagande av Försvarets radioanstalts beslut

2 § Försvarets radioanstalts beslut enligt 5 kap. 2 § att inte lämna information och beslut enligt 5 kap. 5 § i fråga om rättelse, radering, begränsning av behandlingen eller underrättelse till tredje part, får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Paragrafen reglerar överklagande av Försvarets radioanstalts beslut. Övervägandena finns i avsnitt 14.4.1.

Enligt *första stycket* får Försvarets radioanstalts beslut enligt 5 kap. 2 § att inte lämna information och beslut enligt 5 kap. 5 § i fråga om rättelse, radering, begränsning av behandlingen eller underrättelse till tredje part överklagas till allmän förvaltningsdomstol. Uppräkningen är, som framgår av 4 §, uttömmande.

Vilken förvaltningsdomstol som är behörig framgår av 14 § förordningen (1977:937) om allmänna förvaltningsdomstolars behörighet m.m.

Enligt *andra stycket* krävs det prövningstillstånd vid överklagande till kammarrätten.

Överklagande av tillsynsmyndighetens beslut

3 § Tillsynsmyndighetens beslut om föreläggande enligt 6 kap. 5 § första stycket 2 får överklagas till allmän förvaltningsdomstol. När ett beslut överklagas är tillsynsmyndigheten motpart i domstolen.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Paragrafen reglerar överklagande av tillsynsmyndighetens beslut. Övervägandena finns i avsnitt 14.4.2.

Enligt *första stycket* får tillsynsmyndighetens beslut om föreläggande enligt 6 kap. 5 § första stycket 2 överklagas till allmän förvaltningsdomstol. I stycket anges vidare att tillsynsmyndigheten är motpart i domstolen när ett beslut överklagas.

Enligt *andra stycket* krävs prövningstillstånd vid överklagande till kammarrätten.

Överklagandeförbud

4 § Andra beslut enligt denna lag än de som anges i 2 och 3 §§ får inte överklagas.

Paragrafen innehåller ett överklagandeförbud. Övervägandena finns i avsnitt 14.4.1 och 14.4.2.

Av paragrafen framgår att andra beslut enligt lagen än de som anges i 2 och 3 §§ inte får överklagas. Uppräkningen är uttömmande. Någon rätt

att med stöd av förvaltningslagen (2017:900) överklaga andra beslut som Försvarsmakten eller tillsynsmyndigheten enligt lagen finns alltså inte.

Ikraftträdande- och övergångsbestämmelser

1. Denna lag träder i kraft den 1 januari 2022.
2. Genom lagen upphävs lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet.
3. Äldre föreskrifter gäller fortfarande för överklagande av beslut som har meddelats före ikraftträdandet.

Ikraftträdande- och övergångsbestämmelserna behandlas i avsnitt 17.

Enligt *punkten 1* träder lagen i kraft den 1 januari 2022.

Genom *punkten 2* upphävs lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet.

Av *punkten 3* följer att äldre föreskrifter fortfarande gäller för överklagande av beslut som har meddelats före ikraftträdandet. Med äldre föreskrifter avses lagen om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet, förordningen (2007:261) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet, personuppgiftslagen (1998:204) och personuppgiftsförordningen (1998:1191).

19.3 Förslaget till lag om ändring i lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet

1 § I försvarsunderrättelseverksamhet enligt lagen (2000:130) om försvarsunderrättelseverksamhet får den myndighet som regeringen bestämmer (*signalspaningsmyndigheten*) inhämta signaler i elektronisk form vid signalspaning. Signalspaning i försvarsunderrättelseverksamhet får endast ske i de fall regeringen eller en myndighet som anges i 4 § närmare har bestämt inriktningen av signalspaningen.

Signalspaning i försvarsunderrättelseverksamhet får ske endast i syfte att 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 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,
8. främmande makts agerande eller avsikter av väsentlig betydelse för svensk utrikes-, säkerhets- eller försvarspolitik, eller
9. *sådana företeelser som avses i 1–8, men som inte riktas mot Sverige eller rör svenska intressen, om det är nödvändigt för ett samarbete i underrättelsefrågor*

med andra länder och internationella organisationer som signalspaningsmyndigheten deltar i.

Om det är nödvändigt för försvarsunderrättelseverksamheten får signaler i elektronisk form inhämtas vid signalspaning även för att

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

Paragrafen reglerar bl.a. ändamål för signalspaning. Övervägandena finns i avsnitt 15.1.

I *andra stycket 9*, som är ny, anges ett uttryckligt ändamål som medger att signalspaningsmyndigheten får bedriva signalspaning i syfte att kartlägga sådana företeelser som avses i 1–8, men som inte riktas mot Sverige eller rör svenska intressen, om det är nödvändigt för ett samarbete i underrättelsefrågor med andra länder och internationella organisationer som signalspaningsmyndigheten deltar i. Punkten avser det internationella samarbete som sker inom ramen för signalspaningsmyndighetens försvarsunderrättelseverksamhet.

Bedömningen om signalspaning enligt punkten är nödvändig för ett samarbete i underrättelsefrågor som signalspaningsmyndigheten deltar i görs utifrån regeringens bestämmande av samarbetet och inriktning av verksamheten. Har regeringen bestämt att ett samarbete med ett annat land eller en internationell organisation får bedrivas och därtill har inriktat signalspaning enligt 4 § andra stycket är nödvändighetskravet uppfyllt.

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 upptecknin gen förstöras så snart det står klart att sådana signaler har inhämtats. *Kravet på förstöring gäller även i fråga om upptagningar och upptecknin gar som signalspaningsmyndigheten har fått från ett annat land eller en internationell organisation inom ramen för ett internationellt samarbete.*

Första stycket tillämpas inte i fråga om

1. signaler som utväxlas autonomt mellan tekniska system i sådana fall där signalerna inte innehåller personuppgifter, eller

2. signaler som sänds från eller till utländsk militär personal, utländska statsfartyg, statsluftfartyg eller militära fordon.

Paragrafen reglerar förbud mot signalspaning i vissa fall. Övervägandena finns i avsnitt 15.3.

Enligt *första stycket första meningen* 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 upptecknin gen, enligt *andra meningen*, förstöras så snart det står klart att sådana signaler har inhämtats.

Av *första stycket tredje meningen*, som är ny, framgår att kravet på förstöring enligt första och andra meningarna även gäller i fråga om upptagningar eller upptecknin gar som signalspaningsmyndigheten har fått från ett annat land eller en internationell organisation inom ramen för ett internationellt samarbete. Signalspaningsmyndigheten ska således förstöra upptagningar eller upptecknin gar av sådana signaler som ursprungligen

har inhämtats av en utländsk part så snart det står klart att signalerna har inhämtats på ett sätt som inte är tillåtet för signalspaningsmyndigheten.

I *andra stycket*, som är nytt, införs två nya undantag från förbudet i första stycket. Enligt *andra stycket 1* gäller förstöringsskyldigheten inte för signaler som utväxlas autonomt mellan tekniska system i sådana fall där signalerna inte innehåller personuppgifter. Av *andra stycket 2* framgår att förbudet enligt första stycket inte heller gäller för signaler som sänds till eller från utländsk militär personal.

4 § I lagen (2000:130) om försvarsunderrättelseverksamhet finns bestämmelser om regeringens och myndigheters inriktning av sådan verksamhet. Inriktning av signalspaning får anges endast av regeringen, Regeringskansliet, Försvarsmakten, Säkerhetspolisen och Nationella operativa avdelningen i Polismyndigheten.

Regeringen bestämmer inriktningen av *sådan* verksamhet som bedrivs enligt *1 § andra stycket 9* och tredje stycket.

En inriktning av signalspaning får inte avse endast en viss fysisk person.

Paragrafen reglerar inriktning av signalspaningsmyndighetens signalspaning. Övervägandena finns i avsnitt 15.2.

Andra stycket ändras på så sätt att det införs en bestämmelse som innebär att regeringen även ansvarar för att inrikta den signalspaning som får bedrivas för det ändamål som anges 1 § andra stycket 9, dvs. inom ramen för signalspaningsmyndighetens samarbete i underrättelsefrågor med andra länder och internationella organisationer. Regeringen ansvarar således ensam för inriktningen av den signalspaning som signalspaningsmyndigheten får bedriva inom ramen för myndighetens internationella samarbete i försvarsunderrättelse- och utvecklingsverksamheten.

7 § En upptagning eller uppteckning av uppgifter som har inhämtats enligt denna lag *eller som signalspaningsmyndigheten har fått från ett annat land eller en internationell organisation inom ramen för ett internationellt samarbete* ska omgående förstöras om innehållet

1. berör en viss fysisk person och har bedömts sakna betydelse för verksamhet som avses i 1 §,
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. 5 § tryckfrihetsförordningen eller 2 kap. 5 § 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.

Paragrafen reglerar krav på förstöring av uppgifter. Övervägandena finns i avsnitt 15.3.

Första stycket ändras på så sätt att kravet på förstöring även omfattar en upptagning eller uppteckning av uppgifter som signalspaningsmyndigheten har fått från ett annat land eller en internationell organisation inom ramen för ett internationellt samarbete.

12 a § *I lagen (2021:000) om behandling av personuppgifter vid Försvarets radioanstalt finns ytterligare bestämmelser om behandlingen av inhämtade personuppgifter.*

Paragrafen innehåller en upplysning om att det i lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet finns ytterligare bestämmelser om behandlingen av inhämtade personuppgifter. Övervägandena finns i avsnitt 16.

Ändringen innebär att hänvisningen till lagen om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet ersätts med en hänvisning till lagen (2021:000) om behandling av personuppgifter vid Försvarets radioanstalt.

19.4 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 (2021:000) om behandling av personuppgifter vid Försvarsmakten,*
2. *lagen (2021:000) om behandling av personuppgifter vid Försvarets radioanstalt*, eller
3. lagen (2019:1182) om Säkerhetspolisens behandling av personuppgifter.

Paragrafen reglerar undantag från 2 §, vilken utsträcker EU:s dataskyddsförordnings tillämpningsområde. Övervägandena finns i avsnitt 16.

Ändringen innebär att hänvisningarna till 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 ersätts med hänvisningar till lagen om behandling av personuppgifter vid Försvarsmakten respektive lagen om behandling av personuppgifter vid Försvarets radioanstalt.

19.5 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 i verksamhet *enligt lagen (2021:000) om behandling av personuppgifter vid Försvarsmakten.*

Paragrafen reglerar verksamhet som brottsdatalagen inte gäller. Övervägandena finns i avsnitt 16.

Ändringen i *andra stycket* innebär att hänvisningen till lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst ersätts med en hänvisning till lagen om behandling av personuppgifter vid Försvarsmakten. Övriga ändringar är endast språkliga.

Sammanfattning av betänkandet Personuppgiftsbehandlingen vid Försvarsmakten och Försvarets radioanstalt (SOU 2018:63)

Uppdraget

Sedan nuvarande särskilda regler för personuppgiftsbehandling i Försvarsmaktens och Försvarets radioanstalts verksamheter trädde ikraft 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 utredningen 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 och Försvarets radioanstalt 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.

Lagförslagen i betänkandet SOU 2018:63

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.

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.

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 försvarsunderrättelse-

verksamhet 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.

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.

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 uppteckningen 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.

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.

Förteckning över remissinstanserna (betänkandet SOU 2018:63)

Remissvar har lämnats av Datainspektionen, Forum för dataskydd, Försvarets materielverk, Försvarets radioanstalt, Försvarshögskolan, Försvarsmakten, Försvarsunderrättelsedomstolen, Förvaltningsrätten i Stockholm, Inspektionen för strategiska produkter, Juridiska fakultetsstyrelsen vid Lunds universitet, Justitiekanslern, Kustbevakningen, Myndigheten för samhällsskydd och beredskap, Polismyndigheten, Riksarkivet, Statens inspektion för försvarsunderrättelseverksamheten, Sveriges advokatsamfund, Säkerhetspolisen, Tjänstemännens centralorganisation (TCO), Totalförsvarets forskningsinstitut, Tullverket och Åklagarmyndigheten.

Civil Rights Defenders, Fortifikationsverket, Landsorganisationen i Sverige (LO), Officersförbundet, Riksdagens ombudsmän och Sveriges akademikers centralorganisation (SACO) har avstått från att lämna synpunkter på förslagen i betänkandet eller har inte svarat på remissen.

Sammanfattning av betänkandet Försvarets radioanstalts internationella samarbete – en översyn av regelverket (SOU 2020:68)

Uppdraget

Utredningens uppdrag har varit att se över regleringen av Försvarets radioanstalts internationella samarbete i syfte att säkerställa att den möjliggör för Försvarets radioanstalt att bedriva ett internationellt samarbete inom myndighetens försvarsunderrättelse- och utvecklingsverksamhet på ett effektivt och ändamålsenligt sätt, och med tillbörlig hänsyn till enskildas personliga integritet.

Utredningen bedömer att regleringen överlag möjliggör för Försvarets radioanstalt att bedriva ett sådant internationellt samarbete på ett effektivt och ändamålsenligt sätt, och med tillbörlig hänsyn till enskildas integritet. I syfte att göra regleringen än mer effektiv och ändamålsenlig, och samtidigt stärka integritetsskyddet för enskilda, lämnas förslag till ändringar i lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet och i lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet.

Lagen om signalspaning i försvarsunderrättelseverksamhet

En uttrycklig grund för signalspaning vid internationellt samarbete

Utredningen bedömer att den befintliga regleringen är tydlig i fråga om den signalspaning som Försvarets radioanstalt får bedriva inom sitt internationella samarbete som sker i utvecklingsverksamheten. Motsvarande tydlighet bedöms inte föreligga när det gäller Försvarets radioanstalts signalspaning i försvarsunderrättelseverksamhet vid internationellt samarbete. Utredningen föreslår därför att det i lagen om signalspaning i försvarsunderrättelseverksamhet införs en ny bestämmelse som innebär att Försvarets radioanstalt får bedriva signalspaning om myndigheten, inom ramen för sin försvarsunderrättelseverksamhet, bedriver samarbete i underrättelsefrågor med andra länder och internationella organisationer. De ändamål med företeelser för vilka signalspaning får ske inom Försvarets radioanstalts försvarsunderrättelseverksamhet enligt 1 § andra stycket 1–8 lagen om signalspaning i försvarsunderrättelseverksamhet utgör även ramarna för den signalspaning som får bedrivas vid internationellt underrättelsesamarbete, med den skillnaden att det i detta sammanhang inte ställs krav på att företeelserna behöver vara riktade mot Sverige eller röra svenska intressen. Härigenom möjliggörs ett än mer effektivt och ändamålsenligt samarbete som medverkar till att stärka skyddet av Sveriges försvar och säkerhet, samtidigt som det angivna ändamålet innehåller motsvarande företeelser som avses i punkterna 1–8 i bestämmelsen.

Enligt gällande rätt ska Försvarets radioanstalts internationella samarbete inom försvarsunderrättelse- och utvecklingsverksamhet alltid

föregås av ett närmare bestämmande av regeringen enligt lagen (2000:130) om försvarsunderrättelseverksamhet och lagen om signalspaning i försvarsunderrättelseverksamhet. Med hänsyn till detta och till de tydliga utrikes-, säkerhets- och försvarspolitiska aspekter som finns, bör regeringen ensam ansvara för att inrikta den signalspaning som, efter Försvarsunderrättelsedomstolens godkännande, får utföras vid Försvarets radioanstalts internationella samarbete i försvarsunderrättelse- och utvecklingsverksamhet. Av 4 § lagen om signalspaning i försvarsunderrättelseverksamhet följer att regeringen ensam ansvarar för att inrikta Försvarets radioanstalts utvecklingsverksamhet, i vilket det internationella samarbetet på detta område ingår. Utredningen föreslår ett tillägg i nämnda bestämmelse om regeringens inriktningsansvar för Försvarets radioanstalts internationella samarbete i försvarsunderrättelseverksamhet.

Inga ändringsförslag lämnas i fråga om tillstånd, kontroll och tillsyn

Utredningen bedömer att gällande bestämmelser om tillstånd för signalspaning inte behöver ändras med anledning av Försvarets radioanstalts internationella samarbete i försvarsunderrättelse- och utvecklingsverksamheten i sig eller med anledning av utredningens förslag. Detta gäller även för bestämmelserna om kontroll och tillsyn.

Uttryckliga bestämmelser om förstöring av mottagna uppgifter

Utredningen föreslår att det av lagen om signalspaning i försvarsunderrättelseverksamhet ska framgå att den förstöringsskyldighet med angivna undantag som följer av 2 a § och 7 § även ska gälla för sådana upptagningar och uppteckningar som Försvarets radioanstalt har fått från ett annat land eller en internationell organisation inom ramen för ett internationellt samarbete.

Lagen om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet

Personuppgifter får behandlas vid internationellt samarbete

Gällande lagstiftning ger ett stöd för Försvarets radioanstalt att behandla personuppgifter inom myndighetens internationella samarbete i försvarsunderrättelse- och utvecklingsverksamheten. Med beaktande av detta, och att det i betänkandet Behandlingen av personuppgifter vid Försvarsmakten och Försvarets radioanstalt (SOU 2018:63) föreslås en ny lag och förordning för Försvarets radioanstalts behandling av personuppgifter inom bl.a. myndighetens försvarsunderrättelse- och utvecklingsverksamhet, ser utredningen inte skäl att föreslå någon ny ändamålsbestämmelse för Försvarets radioanstalts behandling av personuppgifter inom myndighetens internationella samarbete. Utredningen ser inte heller att det behöver införas någon ny typ av uppgiftssamling med anledning av Försvarets radioanstalts internationella samarbete.

Precisering av villkoren för överföring av personuppgifter utomlands

Utredningen föreslår att förutsättningarna för att överföra personuppgifter till ett annat land eller en internationell organisation preciseras. I lagen om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet föreslås ett antal villkor som ska vara uppfyllda för att Försvarets radioanstalt ska få överföra personuppgifter till ett annat land eller en internationell organisation. Samtliga villkor måste vara uppfyllda för att en överföring av personuppgifter ska vara tillåten. Villkoren innebär att Försvarets radioanstalt endast får överföra personuppgifter till ett annat land eller en internationell organisation om mottagaren är ett annat lands underrättelse- eller säkerhetstjänst eller ett underrättelse- eller säkerhetsorgan i en internationell organisation. Liksom redan gäller i dag ska överföring av personuppgifter endast få ske om sekretess inte hindrar det. Avslutningsvis ska en viss skyddsnivå föreligga hos mottagaren för att personuppgifter ska kunna överföras till ett annat land eller en internationell organisation. Det åvilar Försvarets radioanstalt att bedöma alla omständigheter kring överföringen och komma till slutsatsen att skyddsåtgärderna är tillräckliga. Exempel på sådant som kan vägas in kan bl.a. vara åtaganden att inte sprida personuppgifterna vidare eller att inte använda personuppgifterna efter viss tidpunkt.

Förslagens konsekvenser

Ekonomiska konsekvenser

Förslagen medför inte några kostnadsökningar för Försvarets radioanstalt, Försvarsunderrättelsedomstolen eller Statens inspektion för försvarsunderrättelseverksamheten, eller i övrigt för det allmänna. Förslagen medför inte heller några kostnadsökningar för enskilda.

Konsekvenser för den personliga integriteten

Förslagen om förstöringsskyldighet av mottagna uppgifter och den föreslagna lagändringen avseende Försvarets radioanstalts behandling av personuppgifter stärker skyddet för enskildas personliga integritet.

Övriga konsekvenser

Utredningens förslag i övrigt bedöms inte få några konsekvenser av de slag som anges i kommittéförordningen (1998:1474).

Lagförslagen i betänkandet SOU 2020:68

Förslag till lag om ändring i lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet

Härigenom föreskrivs att 1 kap. 17 § lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 kap.	
17 §	
Personuppgifter som behandlas med stöd av denna lag får föras över till andra länder eller *mellanfolkliga* organisationer endast *om sekretess inte hindrar det och* det är nödvändigt för att Försvarets radioanstalt *skall* 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 verksamheten vid Försvarets radioanstalt.*	Personuppgifter som behandlas med stöd av denna lag får föras över till andra länder eller *internationella* organisationer endast om det är nödvändigt för att Försvarets radioanstalt *ska* kunna fullgöra sina uppgifter inom ramen för det internationella försvarsunderrättelse- och säkerhetssamarbetet *och* *1. överföringen riktas till en utländsk underrättelse- eller säkerhetstjänst, eller ett underrättelse- eller säkerhetsorgan i en internationell organisation,* *2. sekretess inte hindrar en överföring, och* *3. mottagaren garanterar tillräckligt skydd för personuppgifterna.* *Regeringen får meddela föreskrifter om att överföring får ske även i andra fall än som anges i första stycket 1.* *Regeringen får också besluta om sådan överföring i ett enskilt fall.*

Denna lag träder i kraft den 1 januari 2022.

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

Härigenom föreskrivs att 1, 2 a, 4 och 7 §§ lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 §[1]	
I försvarsunderrättelseverksamhet enligt lagen (2000:130) om försvarsunderrättelseverksamhet får den myndighet som regeringen bestämmer (*signalspaningsmyndigheten*) inhämta signaler i elektronisk form vid signalspaning. Signalspaning i försvarsunderrättelseverksamhet får endast ske i de fall regeringen eller en myndighet som anges i 4 § närmare har bestämt inriktningen av signalspaningen.	
Signalspaning i försvarsunderrättelseverksamhet får ske endast i syfte att 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 och annan grov gränsöverskridande brottslighet som kan hota väsentliga nationella intressen,	
4. utveckling och spridning av massförstörelsevapen, krigs-materiel 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 underrättelse-verksamhet mot svenska intressen, *eller*	7. främmande underrättelse-verksamhet mot svenska intressen,
8. främmande makts agerande eller avsikter av väsentlig betydelse för svensk utrikes-, säkerhets- eller försvarspolitik.	8. främmande makts agerande eller avsikter av väsentlig betydelse för svensk utrikes-, säkerhets- eller försvarspolitik*, eller*
	9. sådana företeelser som avses i punkterna 1–8, men inte riktas mot Sverige eller rör svenska intressen, om det är nödvändigt för ett samarbete i underrättelsefrågor med andra länder och internationella organisationer som signalspaningsmyndigheten deltar i.
Om det är nödvändigt för försvarsunderrättelseverksamheten får signaler i elektronisk form inhämtas vid signalspaning även för att	

[1] Senaste lydelse 2009:967.

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

2. fortlöpande utveckla den teknik och metodik som behövs för att bedriva verksamhet enligt denna lag.

2 a §[2]

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.	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. *Kravet på förstöring gäller även i fråga om upptagningar och uppteckningar som signalspaningsmyndigheten har fått från ett annat land eller en internationell organisation inom ramen för ett internationellt samarbete.*

Första stycket tillämpas inte i fråga om signaler mellan sändare och mottagare på utländska statsfartyg, statsluftfartyg eller militära fordon.

4 §[3]

I lagen (2000:130) om försvarsunderrättelseverksamhet finns bestämmelser om regeringens och myndigheters inriktning av sådan verksamhet. Inriktning av signalspaning får anges endast av regeringen, Regeringskansliet, Försvarsmakten, Säkerhetspolisen och Nationella operativa avdelningen i Polismyndigheten.

Regeringen bestämmer inriktningen av *den* verksamhet som bedrivs enligt 1 § tredje stycket.	Regeringen bestämmer inriktningen av *sådan* verksamhet som bedrivs enligt 1 § *andra stycket 9 och* tredje stycket.

En inriktning av signalspaningen får inte avse endast en viss fysisk person.

7 §[4]

En upptagning eller uppteckning av uppgifter som har inhämtats enligt denna lag ska omgående förstöras om innehållet	En upptagning eller uppteckning av uppgifter som har inhämtats enligt denna lag *eller som signalspaningsmyndigheten har fått från ett annat land eller en internationell organisation inom ramen för ett internationellt*

[2] Senaste lydelse 2009:967.
[3] Senaste lydelse 2014:691.
[4] Senaste lydelse 2018:1918.

samarbete ska omgående förstöras om innehållet

1. berör en viss fysisk person och har bedömts sakna betydelse för verksamhet som avses i 1 §,

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. 5 § tryckfrihetsförordningen eller 2 kap. 5 § 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.

Denna lag träder i kraft den 1 januari 2022.

Förteckning över remissinstanserna (betänkandet SOU 2020:68)

Remissvar har lämnats av Civil Rights Defenders, Försvarets radioanstalt, Försvarsmakten, Försvarsunderrättelsedomstolen, Förvaltningsrätten i Stockholm, Integritetsskyddsmyndigheten (tidigare Datainspektionen), Justitiekanslern, Polismyndigheten, Riksarkivet, Statens inspektion för försvarsunderrättelseverksamheten, Sveriges advokatsamfund och Säkerhetspolisen.

Amnesty International, Forum för dataskydd, Lunds universitet och Riksdagens ombudsmän har avstått från att lämna synpunkter på förslagen i betänkandet eller har inte svarat på remissen.

Synpunkter har även lämnats av Centrum för rättvisa och Säkerhets- och försvarsföretagen.

Lagrådsremissens lagförslag

Förslag till lag 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 i verksamhet som rör Sveriges försvar och säkerhet.

3 § Lagen gäller vid sådan behandling av personuppgifter som är helt eller delvis automatiserad. Den gäller också personuppgifter som ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

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

Ord och uttryck i lagen

5 § I denna lag används följande ord och uttryck.

Ord och 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, samman-

	föring, 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 identifiering av personen i fråga.
Dataskyddsombud	En fysisk person som utses av den personuppgiftsansvarige för att självständigt kontrollera att personuppgifter behandlas författningsenligt och på ett korrekt sätt.
Genetiska uppgifter	Personuppgifter som rör en persons nedärvda eller förvärvade genetiska kännetecken och som framför allt härrör från analys av ett spår av eller ett biologiskt prov från personen i fråga.
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 behandlar personuppgifter för den personuppgiftsansvariges räkning.
Registrerad	Den fysiska person som personuppgiften gäller.
Tredje part	Någon annan än – den registrerade, – den 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.

Personuppgiftsansvar

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

2 kap. Behandling av personuppgifter

Grundläggande krav på behandlingen

Krav på ändamål

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

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

Försvar och säkerhet

2 § 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, kollektivavtal eller annat avtal, eller ett särskilt beslut där regeringen har gett myndigheten i uppdrag att utföra uppgiften.

För Försvarsmaktens behandling av personuppgifter i myndighetens försvarsunderrättelseverksamhet och militära säkerhetstjänst gäller i stället 3–8 §§.

Försvarsunderrättelseverksamhet

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

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

Första stycket gäller endast om inte något annat följer av denna lag eller en förordning som regeringen har meddelat i anslutning till lagen.

5 § 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.

6 § Personuppgifter får behandlas för de ändamål som anges i 5 § endast om

1. personuppgifterna 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 enligt motsvarande äldre föreskrifter,
2. personuppgifterna är nödvändiga för att kartlägga underrättelseverksamhet som riktas mot Försvarsmakten och dess säkerhetsintressen,
3. personuppgifterna är nödvändiga för att kartlägga annan säkerhetshotande verksamhet än som avses i 1 och som innefattar brott eller åsidosättande av skyldigheter i anställning hos Försvarsmakten, och det finns särskilda skäl till att uppgiften ska behandlas,
4. en person har lämnat uppgifter om säkerhetshotande verksamhet och personuppgifterna är nödvändiga för att bedöma personens trovärdighet, eller
5. personuppgifterna avser information som har framkommit i samband med säkerhetsprövning enligt säkerhetsskyddslagen (2018:585) eller i annat fall är nödvändiga för att utföra en uppgift som rör säkerhetsskydd.

7 § Personuppgifter som behandlas enligt 6 § ska förses med upplysning om på vilken av de angivna grunderna uppgiften behandlas.

Om behandlingen av en personuppgift motiveras av något annat än ett antagande om att en person 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 en 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 ett sådant antagande inte finns.

Personuppgifter som behandlas enligt 6 § 1, 2 eller 3 ska i förekommande fall förses med en upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak.

8 § Trots bestämmelserna i 6 och 7 §§ 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 6 § 1, 2 eller 3 tillämpas.

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

Övriga ändamål

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

10 § Personuppgifter som utgör allmänt tillgänglig information får behandlas om det är nödvändigt för den verksamhet som anges i 2, 3 och 5 §§.

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

12 § Försvarsmakten får behandla personuppgifter om lagöverträdelser om det är nödvändigt för myndighetens verksamhet.

Författningsenlig och korrekt behandling

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

Personuppgifternas kvalitet

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

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 personuppgifter behandlas får de dock kompletteras med sådana uppgifter som avses i första stycket, om det är absolut nödvändigt för ändamålen med behandlingen.

16 § Biometriska uppgifter får behandlas endast om det är absolut nödvändigt för ändamålen med 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 ändamålen med behandlingen. Detsamma gäller biometriska uppgifter.

Personnummer och samordningsnummer

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

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

Om den registrerade har lämnat sitt samtycke eller offentliggjort personuppgifterna

19 § Trots 15, 16 och 18 §§ får andra personuppgifter än genetiska uppgifter behandlas, om den registrerade har lämnat sitt uttryckliga samtycke eller på ett tydligt sätt har offentliggjort uppgifterna.

Behandling av personuppgifter i vissa fall

20 § Hantering av information som innebär behandling av personuppgifter ska inte anses oförenlig med bestämmelserna i 1–3, 5, 6, 8, 12–16 och 18 §§ i det skede av behandlingen då det inte har kunnat fastställas vilka personuppgifter som informationen innehåller.

Längsta tid som personuppgifter får behandlas

21 § Personuppgifter får inte behandlas under längre tid än vad som behövs med hänsyn till ändamålen med behandlingen.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om att personuppgifter får behandlas under endast viss tid eller fortsätta behandlas för arkivändamål av allmänt intresse eller för vetenskapliga, statistiska eller historiska ändamål.

Regeringen eller den myndighet som regeringen bestämmer får också besluta om sådan behandling i ett enskilt fall.

Överföring av personuppgifter utomlands

22 § Personuppgifter som behandlas med stöd av denna lag får föras över till ett annat land eller en internationell organisation 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 med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om att överföring får ske även i andra fall om det är nödvändigt för verksamheten vid Försvarsmakten.

Regeringen får också besluta om sådan överföring i ett enskilt fall.

Utlämnande av personuppgifter

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

Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om begränsning av möjligheten att lämna ut personuppgifter elektroniskt på annat sätt än genom direktåtkomst.

3 kap. Gemensamt tillgängliga personuppgifter

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 om vilka uppgiftssamlingar som får finnas och vilka uppgifter som får behandlas i respektive uppgiftssamling.

Regeringen eller den myndighet som regeringen bestämmer får också besluta om uppgiftssamlingar i ett enskilt fall.

Direktåtkomst

2 § Totalförsvarets plikt- och prövningsverk får medges direktåtkomst till personuppgifter som rör Försvarsmaktens personalförsörjning och krigsorganisation och som är gemensamt tillgängliga.

Totalförsvarets plikt- och prövningsverk har rätt att vid direktåtkomst ta del av de personuppgifter som omfattas av åtkomsten.

3 § Säkerhetspolisen och Försvarets radioanstalt får medges direktåtkomst till personuppgifter som utgör bearbetningsunderlag och analysresultat inom försvarsunderrättelseverksamheten och som finns i uppgiftssamlingar.

Säkerhetspolisen och Försvarets radioanstalt har rätt att vid direktåtkomst ta del av de personuppgifter som omfattas av åtkomsten.

4 § 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 med stöd av 2 kap. 3 § och som finns i uppgiftssamlingar.

Första stycket gäller enbart i den utsträckning som sådan direktåtkomst följer av lag eller förordning eller om regeringen har beslutat om den i ett enskilt fall.

5 § 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 § och som finns i uppgiftssamlingar.

Första stycket gäller enbart i den utsträckning som sådan direktåtkomst följer av lag eller förordning eller om regeringen har beslutat om den i ett enskilt fall.

Direktåtkomst i andra fall

6 § Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om direktåtkomst till gemensamt tillgängliga uppgifter eller uppgiftssamlingar i andra fall än de som anges i 2–5 §§.

Regeringen får också besluta om detta i ett enskilt fall.

Omfattningen av direktåtkomsten

7 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om omfattningen av direktåtkomsten och om behörighet och säkerhet vid sådan åtkomst.

Regeringen får också besluta om detta i ett enskilt fall.

4 kap. Skyldigheter 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 att de registrerades rättigheter skyddas.

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

Säkerheten för personuppgifter

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

Dataskyddsombud

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

5 § Ett dataskyddsombud 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. vara kontaktpunkt för enskilda i frågor som rör Försvarsmaktens behandling av personuppgifter, och
4. vid behov söka vägledning av tillsynsmyndigheten.

Personuppgiftsbiträden

6 § 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 registrerades rättigheter.

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

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

9 § 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.

10 § Försvarsmaktens skyldigheter enligt 2 och 3 §§ gäller även för personuppgiftsbiträden som Försvarsmakten anlitar.

5 kap. Enskildas rättigheter

Rätten till information

Allmän information

1 § Försvarsmakten ska göra följande information allmänt tillgänglig:

1. myndighetens identitet och kontaktuppgifter,
2. uppgifter om dataskyddsombudet,
3. kategorier av ändamål för behandlingen,
4. rätten enligt 3 § att begära att få information om behandling av personuppgifter och att få del av dem, och
5. rätten att begära rättelse, radering eller begränsning av behandlingen enligt 6 §.

Information som ska lämnas om personuppgifterna samlas in från den som uppgifterna avser

2 § Om personuppgifter samlas in från den som uppgifterna avser ska Försvarsmakten, när myndigheten får personuppgifterna, på eget initiativ lämna följande information till den registrerade:

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

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

1. vilka personuppgifter om den sökande som behandlas,
2. varifrån personuppgifterna kommer,
3. ändamålen med behandlingen,
4. mottagare eller kategorier av mottagare av personuppgifterna, även i annat land eller internationella organisationer,
5. hur länge personuppgifterna får behandlas eller, om det inte är möjligt att ange, kriterierna för att fastställa det, och
6. rätten att begära rättelse, radering eller begränsning av behandlingen enligt 6 §.

Ett utlämnande av personuppgifter enligt första stycket behöver inte omfatta sådana 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 om information enligt första stycket ska göras skriftligen hos Försvarsmakten och vara undertecknad av den sökande själv. Informationen 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 enligt 2 och 3 §§ gäller inte i den utsträckning sekretess hindrar att uppgifterna lämnas ut.

Om det gäller sekretess är Försvarsmakten inte skyldig att redovisa skälen för ett beslut enligt första stycket eller ett beslut i fråga om rättelse, radering eller begränsning av behandlingen enligt 6 §.

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

Informationsskyldigheten gäller dock om uppgifterna

1. har lämnats ut till tredje part, med undantag för en myndighet som med stöd av författning utövar tillsyn, kontroll eller revision,
2. behandlas enbart för statistiska ändamål eller arkivändamål av allmänt intresse, eller
3. har behandlats under längre tid än ett år i löpande text som inte har fått sin slutliga utformning.

Rätten till rättelse, radering och begränsning av behandlingen

6 § Försvarsmakten ska på begäran av den registrerade snarast rätta, radera eller begränsa behandlingen av 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 registrerade begär det eller om en mera

betydande skada eller olägenhet för den registrerade 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 §§ och information och uppgifter enligt 3 § ska lämnas utan avgift.

6 kap. Tillsyn

Tillsyn över personuppgiftsbehandlingen

1 § Den myndighet som regeringen bestämmer utövar tillsyn över Försvarsmaktens behandling av personuppgifter enligt denna lag, föreskrifter som har meddelats i anslutning till lagen och beslut med stöd av lagen.

Tillsynsmyndigheten ska, när det är motiverat, ge råd och stöd till Försvarsmakten och personuppgiftsbiträden i frågor som gäller deras skyldigheter enligt lag eller annan författning.

Tillsynsmyndighetens befogenheter

Undersökningsbefogenheter

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. den hjälp 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 motverka den risken.

Tillsynsmyndigheten får besluta om en skriftlig varning för att planerad behandling av personuppgifter riskerar att stå i strid med lag eller annan författning. Detsamma gäller om en 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 på annat sätt 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 fullgöra andra skyldigheter, eller

2. besluta att förelägga Försvarsmakten eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsenlig eller att fullgöra andra skyldigheter.

Om ett föreläggande beslutas 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 registrerade för den skada och kränkning av den personliga integriteten som orsakats av behandling av personuppgifter i strid med denna lag, föreskrifter som har meddelats i anslutning till lagen eller beslut med stöd av lagen.

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

Överklagande

Överklagande av Försvarsmaktens beslut

2 § Försvarsmaktens beslut enligt 5 kap. 2 och 3 §§ att inte lämna information och beslut enligt 5 kap. 6 § i fråga om rättelse, radering, begränsning av behandlingen eller underrättelse till tredje part, får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Överklagande av tillsynsmyndighetens beslut

3 § Tillsynsmyndighetens beslut om föreläggande enligt 6 kap. 4 § första stycket 2 får överklagas till allmän förvaltningsdomstol. När ett beslut överklagas är tillsynsmyndigheten motpart i domstolen.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Överklagandeförbud

4 § Andra beslut enligt denna lag än de som anges i 2 och 3 §§ får inte överklagas.

---

1. Denna lag träder i kraft den 1 januari 2022.

2. Genom lagen upphävs lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst.

3. Äldre föreskrifter gäller fortfarande för överklagande av beslut som har meddelats före ikraftträdandet.

Förslag till lag 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. Den gäller också personuppgifter som ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

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

Ord och uttryck i lagen

5 § I denna lag används följande ord och uttryck.

Ord och 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, samman-

	föring, 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 identifiering av personen i fråga.
Dataskyddsombud	En fysisk person som utses av den personuppgiftsansvarige för att självständigt kontrollera att personuppgifter behandlas författningsenligt och på ett korrekt sätt.
Genetiska uppgifter	Personuppgifter som rör en persons nedärvda eller förvärvade genetiska kännetecken och som framför allt härrör från analys av ett spår av eller ett biologiskt prov från personen i fråga.
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 behandlar personuppgifter för den personuppgiftsansvariges räkning.
Registrerad	Den fysiska person som personuppgiften gäller.
Tredje part	Någon annan än – den registrerade, – den 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.

Personuppgiftsansvar

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

2 kap. Behandling av personuppgifter

Grundläggande krav på behandlingen

Krav på ändamål

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

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

Försvarsunderrättelseverksamhet

2 § 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.

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

Första stycket gäller endast om inte något annat följer av denna lag eller en förordning som regeringen har meddelat i anslutning till lagen.

4 § Personuppgifter som behandlas med stöd av 2 och 3 §§ 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 5 §,
4. i informationssäkerhetsverksamheten för de ändamål som anges i 7 §, eller

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

Utvecklingsverksamhet

5 § 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.

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

1. med anledning av samverkan med annan i fråga om 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 2 och 3 §§,
4. i informationssäkerhetsverksamheten för de ändamål som anges i 7 §, eller
5. för att biträda andra myndigheter i den utsträckning det följer av lag eller förordning eller om regeringen har beslutat om det i ett enskilt fall.

Informationssäkerhetsverksamhet

7 § 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 beslut av regeringen i ett enskilt fall.

8 § Personuppgifter som behandlas med stöd av 7 § 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 har beslutat om det i ett enskilt fall,
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 5 §.

Övriga ändamål

9 § Personuppgifter som utgör allmänt tillgänglig information får behandlas av Försvarets radioanstalt om det är nödvändigt för de ändamål som anges i 2, 3, 5 och 7 §§.

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

Författningsenlig och korrekt behandling

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

Personuppgifternas kvalitet

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

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

13 § 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 personuppgifter behandlas får de dock kompletteras med sådana uppgifter som avses i första stycket, om det är absolut nödvändigt för ändamålen med behandlingen.

14 § Biometriska uppgifter får behandlas endast om det är absolut nödvändigt för ändamålen för behandlingen.

Genetiska uppgifter får inte behandlas.

15 § 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 ändamålen med behandlingen. Detsamma gäller biometriska uppgifter.

Personnummer och samordningsnummer

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

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

Om den registrerade har offentliggjort personuppgifterna

17 § Trots 13, 14 och 16 §§ får andra personuppgifter än genetiska uppgifter behandlas, om den registrerade på ett tydligt sätt har offentliggjort uppgifterna.

Behandling av personuppgifter i vissa fall

18 § Hantering av information som innebär behandling av personuppgifter ska inte anses oförenlig med bestämmelserna i 1, 2, 5, 7, 9, 11–14 och 16 §§ i det skede av behandlingen då det inte har kunnat fastställas vilka personuppgifter som informationen innehåller.

Längsta tid som personuppgifter får behandlas

19 § Personuppgifter får inte behandlas under längre tid än vad som behövs med hänsyn till ändamålen med behandlingen.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om att personuppgifter får behandlas under endast viss tid eller fortsätta behandlas för arkivändamål av allmänt intresse eller för vetenskapliga, statistiska eller historiska ändamål.

Regeringen eller den myndighet som regeringen bestämmer får också besluta om sådan behandling i ett enskilt fall.

Överföring av personuppgifter utomlands

20 § Personuppgifter som behandlas med stöd av denna lag får föras över till ett annat land eller en internationell organisation endast om det är nödvändigt för att Försvarets radioanstalt ska kunna fullgöra sina uppgifter inom ramen för det internationella försvarsunderrättelse- och säkerhetssamarbetet och

1. överföringen riktas till en utländsk underrättelse- eller säkerhetstjänst, eller ett underrättelse- eller säkerhetsorgan i en internationell organisation,
2. sekretess inte hindrar en överföring, och
3. mottagaren garanterar tillräckligt skydd för personuppgifterna.

Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om att överföring får ske även i andra fall än som anges i första stycket 1.

Regeringen får också besluta om sådan överföring i ett enskilt fall.

Utlämnande av personuppgifter

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

3 kap. Gemensamt tillgängliga personuppgifter

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. 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 om vilka uppgiftssamlingar som får finnas och vilka uppgifter som får behandlas i respektive uppgiftssamling.

Regeringen eller den myndighet som regeringen bestämmer får också besluta om uppgiftssamlingar i ett enskilt fall.

Direktåtkomst

Försvarsunderrättelseverksamhet

2 § Säkerhetspolisen och Försvarsmakten får medges direktåtkomst till personuppgifter som utgör analysresultat inom försvarsunderrättelseverksamheten och som finns i uppgiftssamlingar.

Säkerhetspolisen och Försvarsmakten har rätt att vid direktåtkomst ta del av de personuppgifter som omfattas av åtkomsten.

3 § Om det behövs för samarbetet mot terrorism eller för annat internationellt säkerhetssamarbete, får en utländsk underrättelse- eller säkerhetstjänst medges direktåtkomst till personuppgifter som behandlas med stöd av 2 kap. 2 § och som finns i uppgiftssamlingar.

Första stycket gäller enbart i den utsträckning som sådan direktåtkomst följer av lag eller förordning eller om regeringen har beslutat om den i ett enskilt fall.

Informationssäkerhetsverksamhet

4 § Om det behövs för samarbetet mot it-relaterade hot mot samhällsviktiga system, får en utländsk organisation inom informationssäkerhetsområdet medges direktåtkomst till personuppgifter som behandlas med stöd av 2 kap. 7 § och som finns i uppgiftssamlingar.

Första stycket gäller enbart i den utsträckning som sådan direktåtkomst följer av lag eller förordning eller om regeringen har beslutat om den i ett enskilt fall.

Direktåtkomst i andra fall

5 § Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om direktåtkomst till uppgiftssamlingar i andra fall än de som anges i 2–4 §§.

Regeringen får också besluta om detta i ett enskilt fall.

Omfattningen av direktåtkomsten

6 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om omfattningen av direktåtkomsten och om behörighet och säkerhet vid sådan åtkomst.

Regeringen får också besluta om detta i ett enskilt fall.

4 kap. Skyldigheter 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 att de registrerades rättigheter skyddas.

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

Säkerheten för personuppgifter

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

Dataskyddsombud

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

5 § Ett dataskyddsombud 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. vara kontaktpunkt för enskilda i frågor som rör Försvarets radioanstalts behandling av personuppgifter, och
4. vid behov söka vägledning av tillsynsmyndigheten.

Personuppgiftsbiträden

6 § 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 registrerades rättigheter.

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

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

9 § 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.

10 § Försvarets radioanstalts skyldigheter enligt 2 och 3 §§ gäller även för personuppgiftsbiträden som Försvarets radioanstalt anlitar.

5 kap. Enskildas rättigheter

Rätten till information

Allmän information

1 § Försvarets radioanstalt ska göra följande information allmänt tillgänglig:

1. myndighetens identitet och kontaktuppgifter,
2. uppgifter om dataskyddsombudet,
3. kategorier av ändamålen med behandlingen,
4. rätten enligt 2 § att begära att få information om behandling av personuppgifter och att få del av dem, och
5. rätten att begära rättelse, radering eller begränsning av behandlingen enligt 5 §.

Information som ska lämnas efter begäran

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

1. vilka personuppgifter om den sökande som behandlas,
2. varifrån personuppgifterna kommer,
3. ändamålen med behandlingen,
4. mottagare eller kategorier av mottagare av personuppgifterna, även i annat land eller internationella organisationer,
5. hur länge personuppgifterna får behandlas eller, om det inte är möjligt att ange, kriterierna för att fastställa det, och
6. rätten att begära rättelse, radering eller begränsning av behandlingen enligt 5 §.

Ett utlämnande av personuppgifter enligt första stycket behöver inte omfatta sådana 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 om information enligt första stycket ska göras skriftligen hos Försvarets radioanstalt och vara undertecknad av den sökande själv. Informationen 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.

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

Om det gäller sekretess är Försvarets radioanstalt inte skyldig att redovisa skälen för ett beslut enligt första stycket eller ett beslut i fråga om rättelse, radering eller begränsning av behandlingen enligt 5 §.

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

Informationsskyldigheten gäller dock om uppgifterna

1. har lämnats ut till tredje part, med undantag för en myndighet som med stöd av författning utövar tillsyn, kontroll eller revision,
2. behandlas enbart för statistiska ändamål eller arkivändamål av allmänt intresse, eller
3. har behandlats under längre tid än ett år i löpande text som inte har fått sin slutliga utformning.

Rätten till rättelse, radering och begränsning av behandlingen

5 § Försvarets radioanstalt ska på begäran av den registrerade snarast rätta, radera eller begränsa behandlingen av 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 registrerade begär det eller om en mera betydande skada eller olägenhet för den registrerade 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 § och information och uppgifter enligt 2 § ska lämnas utan avgift.

6 kap. Tillsyn

Tillsyn över personuppgiftsbehandlingen

1 § Den myndighet som regeringen bestämmer utövar tillsyn över Försvarets radioanstalts behandling av personuppgifter enligt denna lag, föreskrifter som har meddelats i anslutning till lagen och beslut med stöd av lagen.

Tillsynsmyndigheten ska, när det är motiverat, ge råd och stöd till Försvarets radioanstalt och personuppgiftsbiträden i frågor som gäller deras skyldigheter enligt lag eller annan författning.

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.

Tillsynsmyndighetens befogenheter

Undersökningsbefogenheter

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. den hjälp 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 motverka den risken.

Tillsynsmyndigheten får besluta om en skriftlig varning för att planerad behandling av personuppgifter riskerar att stå i strid med lag eller annan författning. Detsamma gäller om en 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 på annat sätt 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 fullgöra andra skyldigheter, eller
2. besluta att förelägga Försvarets radioanstalt eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsenlig eller att fullgöra andra skyldigheter.

Om ett föreläggande beslutas 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 registrerade för den skada och kränkning av den personliga integriteten som orsakats av

behandling av personuppgifter i strid med denna lag, föreskrifter som har meddelats i anslutning till lagen eller beslut med stöd av lagen.

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

Överklagande

Överklagande av Försvarets radioanstalts beslut

2 § Försvarets radioanstalts beslut enligt 5 kap. 2 § att inte lämna information och beslut enligt 5 kap. 5 § i fråga om rättelse, radering, begränsning av behandlingen eller underrättelse till tredje part, får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Överklagande av tillsynsmyndighetens beslut

3 § Tillsynsmyndighetens beslut om föreläggande enligt 6 kap. 5 § första stycket 2 får överklagas till allmän förvaltningsdomstol. När ett beslut överklagas är tillsynsmyndigheten motpart i domstolen.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Överklagandeförbud

4 § Andra beslut enligt denna lag än de som anges i 2 och 3 §§ får inte överklagas.

---

1. Denna lag träder i kraft den 1 januari 2022.

2. Genom lagen upphävs lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet.

3. Äldre föreskrifter gäller fortfarande för överklagande av beslut som har meddelats före ikraftträdandet.

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

Härigenom föreskrivs att 1, 2 a, 4, 7 och 12 a §§ lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet ska ha följande lydelser.

Nuvarande lydelse	*Föreslagen lydelse*
1 §[1]	
I försvarsunderrättelseverksamhet enligt lagen (2000:130) om försvarsunderrättelseverksamhet får den myndighet som regeringen bestämmer (*signalspaningsmyndigheten*) inhämta signaler i elektronisk form vid signalspaning. Signalspaning i försvarsunderrättelseverksamhet får endast ske i de fall regeringen eller en myndighet som anges i 4 § närmare har bestämt inriktningen av signalspaningen.	
Signalspaning i försvarsunderrättelseverksamhet får ske endast i syfte att 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 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*	7. främmande underrättelseverksamhet mot svenska intressen,
8. främmande makts agerande eller avsikter av väsentlig betydelse för svensk utrikes-, säkerhets- eller försvarspolitik.	8. främmande makts agerande eller avsikter av väsentlig betydelse för svensk utrikes-, säkerhets- eller försvarspolitik, *eller*
	9. sådana företeelser som avses i 1–8, men som inte riktas mot Sverige eller rör svenska intressen, om det är nödvändigt för ett samarbete i underrättelsefrågor med andra länder och internationella organisationer som signalspaningsmyndigheten deltar i.
Om det är nödvändigt för försvarsunderrättelseverksamheten får signaler i elektronisk form inhämtas vid signalspaning även för att	

[1] Senaste lydelse 2009:967.

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

2. fortlöpande utveckla den teknik och metodik som behövs för att bedriva verksamhet enligt denna lag.

2 a §[2]

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.

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. *Kravet på förstöring gäller även i fråga om upptagningar och uppteckningar som signalspaningsmyndigheten har fått från ett annat land eller en internationell organisation inom ramen för ett internationellt samarbete.*

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

1. signaler som utväxlas autonomt mellan tekniska system i sådana fall där signalerna inte innehåller personuppgifter, eller

2. *signaler som sänds från eller till utländsk militär personal,* utländska statsfartyg, statsluftfartyg eller militära fordon.

4 §[3]

I lagen (2000:130) om försvarsunderrättelseverksamhet finns bestämmelser om regeringens och myndigheters inriktning av sådan verksamhet. Inriktning av signalspaning får anges endast av regeringen, Regeringskansliet, Försvarsmakten, Säkerhetspolisen och Nationella operativa avdelningen i Polismyndigheten.

Regeringen bestämmer inriktningen av *den* verksamhet som bedrivs enligt 1 § tredje stycket.

Regeringen bestämmer inriktningen av *sådan* verksamhet som bedrivs enligt 1 § *andra stycket 9 och* tredje stycket.

En inriktning av signalspaningen får inte avse endast en viss fysisk person.

[2] Senaste lydelse 2009:967.
[3] Senaste lydelse 2014:691.

7 §[4]

En upptagning eller uppteckning av uppgifter som har inhämtats enligt denna lag ska omgående förstöras om innehållet	En upptagning eller uppteckning av uppgifter som har inhämtats enligt denna lag *eller som signalspaningsmyndigheten har fått från ett annat land eller en internationell organisation inom ramen för ett internationellt samarbete* ska omgående förstöras om innehållet

1. berör en viss fysisk person och har bedömts sakna betydelse för verksamhet som avses i 1 §,

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. 5 § tryckfrihetsförordningen eller 2 kap. 5 § 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.

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 *(2021:000)* om behandling av personuppgifter *vid Försvarets radioanstalt* finns ytterligare bestämmelser om behandlingen av inhämtade personuppgifter.

Denna lag träder i kraft den 1 januari 2022.

[4] Senaste lydelse 2018:1918.

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

Härigenom föreskrivs i fråga om lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning[1]

dels att punkt 3 i ikraftträdande- och övergångsbestämmelserna ska upphöra att gälla,

dels att 1 kap. 3 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 kap.	
3 §[2]	
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 (2021:000) om behandling av personuppgifter vid Försvarsmakten*,
2. *lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet*, eller	2. *lagen (2021:000) om behandling av personuppgifter vid Försvarets radioanstalt*, eller
3. lagen (2019:1182) om Säkerhetspolisens behandling av personuppgifter.	

Denna lag träder i kraft den 1 januari 2022.

[1] Senaste lydelse av punkt 3 i ikraftträdande- och övergångsbestämmelserna 2020:152.
[2] Senaste lydelse 2019:1186.

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 i verksamhet *enligt lagen (2021:000) om behandling av personuppgifter vid Försvarsmakten*.

Denna lag träder i kraft den 1 januari 2022.

Lagrådets yttrande

Utdrag ur protokoll vid sammanträde 2021-06-24

Närvarande: F.d. justitierådet Eskil Nord samt justitieråden Inga-Lill Askersjö och Petter Asp

Behandling av personuppgifter vid Försvarsmakten och Försvarets radioanstalt

Enligt en lagrådsremiss den 3 juni 2021 har regeringen (Försvarsdepartementet) beslutat inhämta Lagrådets yttrande över förslag till

1. lag om behandling av personuppgifter vid Försvarsmakten,
2. lag om behandling av personuppgifter vid Försvarets radioanstalt,
3. lag om ändring i lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet,
4. lag om ändring i lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning,
5. lag om ändring i brottsdatalagen (2018:1177).

Förslagen har inför Lagrådet föredragits av ämnesrådet Mikael Andersson.

Förslagen föranleder följande yttrande.

Förslaget till lag om behandling av personuppgifter vid Försvarsmakten

1 kap. 6 §

I paragrafen anges att Försvarsmakten är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför. I författningskommentaren förklaras att det innebär att Försvarsmakten är ansvarig även för den personuppgiftsbehandling som utförs av personuppgiftsbiträden som myndigheten anlitar. Det bör enligt Lagrådet framgå direkt av lagen. Det gäller särskilt med beaktande av att lagstiftningen på näraliggande områden är utformad så att detta framgår (jfr 1 kap. 6 § lagen om Säkerhetspolisens behandling av personuppgifter).

Lagrådet föreslår att paragrafen ges följande lydelse.

Försvarsmakten är personuppgiftsansvarig för all behandling av personuppgifter som myndigheten utför, som utförs under myndighetens ledning eller på dess vägnar.

2 kap. 2 §

Regleringen i paragrafen väcker ett antal frågor om förhållandet mellan bestämmelserna i denna paragraf och andra paragrafer i lagen. Enligt författningskommentaren är avsikten med regleringen i aktuell paragraf att ange vissa ändamål för Försvarsmaktens personuppgiftsbehandling. Enligt ordalydelsen i *första stycket* får personuppgifter behandlas om det är

nödvändigt för att planera, förbereda och genomföra verksamhet som rör dels Sveriges försvar och säkerhet (punkt 1), dels internationellt försvars- och säkerhetssamarbete (punkt 2). Redan här inställer sig frågan om förhållandet till bestämmelsen om lagens tillämpningsområde i 1 kap. 2 §. I den sistnämnda paragrafen anges nämligen att lagen gäller vid Försvarsmaktens behandling av personuppgifter i verksamhet som rör Sveriges försvar och säkerhet, dvs. endast den verksamhet som anges i punkt 1 i aktuell paragraf. Det framstår således som om ”internationellt försvars- och säkerhetssamarbete” inte omfattas av lagens tillämpningsområde. Vid föredragningen har emellertid förklarats att ”internationellt försvars- och säkerhetssamarbete” är avsett att ingå i ”Sveriges försvar och säkerhet” i den mening det sistnämnda begreppet har i 1 kap. 2 §. Detta innebär att det antingen är så att ”Sveriges försvar och säkerhet” har en annan betydelse i 1 kap. 2 § än i 2 kap. 2 § eller att den andra punkten i 2 kap. 2 § är helt onödig och missvisande. Oavsett vilket riskerar regleringen att skapa osäkerhet vid tillämpningen. Redan det sagda gör att det valda regleringssättet inte är godtagbart. Lagrådet ifrågasätter också behovet av att i aktuell paragraf dela upp Försvarsmaktens verksamhet i två delar. Uppdelningen synes inte ha någon betydelse för övrig reglering i lagen. Eftersom uppdelningen endast leder till att regleringen blir förvirrande vore det bättre att i paragrafen enbart ange ”Sveriges försvar och säkerhet” och i författningskommentaren redogöra för vad som ingår i den verksamheten, t.ex. internationellt försvars- och säkerhetssamarbete.

Lagrådet föreslår därför att punkt 2 utgår i första stycket.

Om det inte förhåller sig på sätt som anges ovan måste tillämpningsområdet i 1 kap. 2 § utvidgas till att omfatta mer än enbart ”Sveriges försvar och säkerhet” och lagstiftningen i övrigt anpassas så att det klart framgår vilka verksamheter som, utöver Sveriges försvar och säkerhet, bedrivs inom Försvarsmakten.

I *andra stycket* i aktuell paragraf föreskrivs att Försvarsmaktens uppgift att bedriva sådan verksamhet som anges i första stycket ska följa av lag, förordning, kollektivavtal eller annat avtal eller ett särskilt beslut där regeringen har gett myndigheten i uppdrag att utföra uppgiften, dvs. det som oftast numera i reglering av personuppgiftsbehandling kallas för rättslig grund. I lagrådsremissen betecknas emellertid också detta som ändamål. Även om det av pedagogiska skäl ibland blir komplicerat att benämna detta som ändamål har Lagrådet i och för sig inget att invända mot den terminologin, men det måste då bli tydligt hur just detta ”ändamål” förhåller sig till andra ändamål som föreskrivs. Om det som föreskrivs i andra stycket är uppfyllt har Försvarsmakten genom den regleringen och punkt 1 i första stycket rätt att behandla uppgifter inom hela sin verksamhet. Enligt tredje stycket anges emellertid att när det gäller försvarsunderrättelseverksamheten och den militära säkerhetstjänsten så gäller *i stället* 3–8 §§. Även beträffande dessa verksamheter har vid föredragningen förklarats att de ingår i ”Sveriges försvar och säkerhet”, men att de bör regleras särskilt. Om Lagrådet uppfattat det rätt så vill man för denna del av Försvarsmaktens verksamhet föreskriva särskilda ändamål. Det kan dock konstateras att bestämmelsen i tredje stycket leder

till att andra stycket (om den rättsliga grunden) inte kommer att gälla för dessa delar. När det gäller försvarsunderrättelseverksamheten så anges i 3 § en särskild lag, men för den militära säkerhetstjänsten saknas en sådan bestämmelse. I sistnämnda fall föreskrivs i 5–8 §§ endast ett antal ändamål som måste vara uppfyllda för att behandlingen ska få ske. Lagrådet utgår dock från att avsikten är att även denna behandling ska ha sådant stöd i lag, förordning m.m. som föreskrivs i andra stycket.

Vid föredragningen har förklarats att regleringen har fått sin utformning närmast av pedagogiska skäl. Man har velat tydliggöra att det rör sig om olika delar av verksamheten, trots att det i grunden är en och samma verksamhet, nämligen ”Sveriges försvar och säkerhet”. Enligt Lagrådets mening har emellertid regleringen tvärtom kommit att bli otydlig och förvirrande.

En mer ändamålsenlig ordning vore att i tredje stycket föreskriva att det i 3–8 §§ finns särskilda ändamål som gäller för den del av Försvarsmaktens verksamhet som avser försvarsunderrättelseverksamheten och den militära säkerhetstjänsten. Om så sker kommer dessa delar av verksamheten inte att exkluderas från aktuell paragraf. Härigenom tillskapas en heltäckande reglering även för dem.

I tredje stycket bör av samma skäl tydliggöras att de ändamål som föreskrivs i 9–12 §§ under rubriken ”Övriga ändamål” inte är skilda från det som föreskrivs i 2 §. Även när det gäller personuppgifts-behandling som sker för dessa ändamål måste det naturligtvis finnas stöd i en rättslig grund.

Lagrådet föreslår att tredje stycket ges följande lydelse.

För Försvarsmaktens behandling av personuppgifter i myndighetens försvarsunderrättelseverksamhet och militära säkerhetstjänst finns särskilda bestämmelser om ändamål i 3–8 §§. I 9–12 §§ finns ytterligare bestämmelser som preciserar ändamålet i denna paragraf.

2 kap. 6 §

Paragrafen innehåller ändamålsbestämmelser för personuppgifts-behandling inom den militära underrättelsetjänsten. I punkt 5 anges att behandling får ske om personuppgifterna avser information som har framkommit i samband med säkerhetsprövning enligt säkerhetsskydds-lagen eller i annat fall är nödvändiga för att utföra en uppgift som rör säkerhetsskydd. Varken av ordalydelsen eller av författningskommentaren går det att utläsa vilka uppgifter som avses. Vid föredragningen har klargjorts att det som avses är uppgifter som är nödvändiga för att genomföra en säkerhetsprövning eller för att utföra en uppgift som rör säkerhetsskydd. Punkten bör omformuleras så att tillämpningsområdet för bestämmelsen inskränks till att omfatta enbart sådana uppgifter.

Punkten 4 bör justeras språkligt och ges en lydelse som samstämmer med övriga punkter i uppräkningen.

Lagrådet föreslår att punkterna 4 och 5 ges följande lydelse.

4. personuppgifterna är nödvändiga för att bedöma om en person som har lämnat uppgifter om säkerhetshotande verksamhet är trovärdig, eller
5. personuppgifterna är nödvändiga för att genomföra säkerhetsprövning enligt säkerhetsskyddslagen (2018:585) eller för att utföra en uppgift som rör säkerhetsskydd.

2 kap. 16 och 17 §§

Bestämmelsen i 17 § reglerar när personuppgifter som avslöjar ras, etniskt ursprung, politiska åsikter m.m. får användas vid sökning. Det får ske om det är absolut nödvändigt för ändamålen med behandlingen. Bestämmelsen i denna paragraf anger inte − som i 16 § − att det ”endast” får ske under den förutsättningen. Eftersom graden av nödvändighet inte är avsedd att skilja sig åt i de båda paragraferna bör de samstämma språkligt. Ordet ”endast” bör därför tillföras i 17 §, alternativt tas bort i 16 §.

Dessutom bör ordet ”för” bytas ut mot ”med hänsyn till” i båda paragraferna. Det sistnämnda återkommer i ett antal paragrafer i lagen som bör justeras på samma sätt.

2 kap. 20 §

I paragrafen anges att en behandling av personuppgifter inte ska anses oförenlig med bestämmelserna i ett antal uppräknade paragrafer, om den sker i ett skede då det inte har kunnat fastställas vilka uppgifter som informationen innehåller. Det saknas en förklaring till varför bestämmelserna i just de uppräknade paragraferna ska omfattas.

Det kan ifrågasättas om undantaget – vilket är fallet enligt ordalydelsen – fullt ut ska vara tillämpligt också i de fall när man vet *att* materialet innehåller personuppgifter och osäkerheten endast gäller *vilka* personuppgifter det är fråga om. En av de mer tveksamma hänvisningarna är den till 2 kap. 2 §, dvs. där det anges att behandlingen måste vara nödvändig för att planera, förbereda och genomföra verksamhet samt att verksamheten som bedrivs ska ha stöd i lag, förordning, m.m. Dessa förutsättningar måste anses vara sådana som ska gälla även om myndigheten ännu inte vet vilka personuppgifter som den behandlar.

Det är således sannolikt att undantaget genom uppräkningen av paragrafer har blivit för omfattande. Eftersom uppräkningen styr vilken behandling som får ske bör det i författningskommentaren klargöras vad varje uppräknad paragraf innebär för rätten att behandla innan det har kunnat fastställas vilka personuppgifter det gäller. Frågan bör övervägas i det fortsatta lagstiftningsarbetet.

2 kap. 22 §

Paragrafen reglerar under vilka förutsättningar överföring av personuppgifter får ske till utlandet. Inledningsvis kan konstateras att underrubriken till paragrafen är missvisande. Det är naturligtvis inte fråga om ”Överföring av personuppgifter utomlands”, vilket närmast låter som om överföringen sker mellan två mottagare utomlands. Rubriken bör i stället lyda ”Överföring av personuppgifter till en mottagare utomlands”.

Enligt första stycket får överföring ske om tre förutsättningar är för handen. För det första ska det gälla en överföring till ett annat land eller en internationell organisation, för det andra får inte sekretess hindra det och för det tredje ska det ske för att Försvarsmakten ska kunna fullgöra sina uppgifter inom ramen för det internationella försvars- och säkerhetssamarbetet. I andra stycket upplyses att regeringen med stöd av 8 kap. 7 § regeringsformen får meddela föreskrifter om att överföring får ske även *i andra fall* om det är nödvändigt för verksamheten vid Försvarsmakten. Vad som avses med andra fall är inte klart. Det är bl.a. oklart vilken eller vilka av de tre förutsättningarna som ”andra fall” syftar på. Detta bör klargöras i författningskommentaren.

2 kap. 23 §

Bestämmelsen har getts en olycklig språklig utformning. Ordalydelsen ger intryck av att personuppgifter får lämnas ut elektroniskt om det inte är olämpligt, men att det inte ställs något sådant krav på lämplighet om utlämnandet sker genom direktåtkomst. När det gäller direktåtkomst gäller emellertid strängare regler som finns i 3 kap. Det gäller dels direkt i lagen föreskrivna inskränkningar, dels − som det upplyses om i 3 kap. 6 och 7 §§ − restriktioner som kan följa av föreskrifter av regeringen eller av den myndighet som regeringen bestämmer. För att detta tydligt ska framgå föreslår Lagrådet att bestämmelsen ges följande lydelse.

Personuppgifter får lämnas ut elektroniskt om det inte är olämpligt. Utlämnande genom direktåtkomst får dock ske endast under de förutsättningar som följer av 3 kap.

3 kap. 2 §

I paragrafen anges under vilka förutsättningar Totalförsvarets plikt- och prövningsverk får medges direktåtkomst till personuppgifter som rör Försvarsmaktens personalförsörjning och krigsorganisation. En av förutsättningarna är att personuppgifterna ska vara gemensamt tillgängliga. Med gemensamt tillgängliga avses enligt 1 § att inte endast ett fåtal personer har tillgång till uppgifterna. Det förefaller besynnerligt att ett krav för att plikt- och prövningsverket ska få direktåtkomst är att fler än ett fåtal personer ska få tillgång till uppgifterna. Personuppgiftsskyddet blir ju nämligen starkare om endast ett fåtal personer får tillgång till dem.

Vid föredragningen har upplysts att begreppet ”gemensamt tillgängliga” avser den egna myndigheten, dvs. att det ska röra sig om uppgifter som fler än ett fåtal på den egna myndigheten har tillgång till. När det som i nu aktuell paragraf handlar om två myndigheter, så inställer sig emellertid frågan om det krävs att uppgifterna är gemensamt tillgängliga hos båda myndigheterna, dvs. både hos den som ger och den som får direktåtkomst. Måste fler än ett fåtal ha tillgång till uppgifterna hos båda myndigheterna för paragrafens tillämpning? Detta bör framgå av paragrafen eller i vart fall tydliggöras i författningskommentaren.

Begreppet ”gemensamt tillgängliga” finns i ett antal paragrafer i lagen och det är väsentligt att det ges samma innebörd i dem alla. Det bör övervägas om det vore lämpligt att ta in en definition av begreppet i katalogen i 1 kap. 5 §.

5 kap. 4 §

Den som registreras har rätt att under vissa förutsättningar kräva att få information om registreringen. Enligt första stycket i aktuell paragraf föreligger dock begränsningar i denna rätt om sekretess hindrar att uppgifterna lämnas ut. Om det gäller sekretess är Försvarsmakten enligt andra stycket inte skyldig att redovisa skälen för ett beslut enligt första stycket.

Det kan inledningsvis konstateras att det inte talas om något beslut i första stycket. Det andra stycket bör alltså formuleras om så att hela beslutssituationen regleras där. Vidare räcker det inte med att det föreligger sekretess för en uppgift. Sekretessregleringen måste också medföra att det på grund av sekretess finns hinder att lämna ut uppgiften till den registrerade. Andra stycket bör omformuleras så att detta klart framgår. Lagrådet föreslår följande lydelse.

> Informationsskyldigheten enligt 2 och 3 §§ gäller inte i den utsträckning sekretess hindrar att uppgifterna lämnas ut till den registrerade.
>
> Om Försvarsmakten med stöd av första stycket beslutar att inte lämna ut uppgifterna är Försvarsmakten inte skyldig att redovisa skälen för beslutet. Detsamma gäller i fråga om rättelse, radering eller begränsning av behandlingen enligt 6 §.

5 kap. 6 §

Paragrafen reglerar Försvarsmaktens skyldighet att rätta, radera eller begränsa behandlingen av personuppgifter. Enligt andra stycket ska Försvarsmakten också underrätta tredje part om åtgärden. Bestämmelsen har av misstag kommit att ge en felaktig bild av vad underrättelsen innebär. Det är även oklart vad ordet ”också” syftar på. Det som avses är att tredje part ska underrättas om att en uppgift som tidigare har lämnats ut till denne därefter har rättats, raderats eller begränsats.

Lagrådet föreslår att andra stycket ges följande lydelse.

Om uppgifterna har lämnats ut till tredje part ska denne underrättas om en åtgärd enligt första stycket om den registrerade begär det eller om en mera betydande skada skulle kunna undvikas genom en underrättelse.

6 kap. 1 §

I första stycket anges att den myndighet som regeringen bestämmer utövar tillsyn över Försvarsmaktens behandling av personuppgifter enligt lagen, föreskrifter som har meddelats i anslutning till lagen och beslut med stöd av lagen. Bestämmelsen skulle kunna läsas så att tillsynen avser själva föreskrifterna och besluten i stället för den behandling som sker enligt dessa. Även de båda sista leden bör därför tillföras ordet ”enligt” och förslagsvis ges följande lydelse.

…enligt föreskrifter som har meddelats i anslutning till lagen och enligt beslut som fattats med stöd av lagen.

6 kap. 4 §

I första stycket anges i två punkter att tillsynsmyndigheten får försöka förmå respektive besluta att förelägga ”Försvarsmakten eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsenlig eller att fullgöra andra skyldigheter”. Eftersom punkterna består av inte mindre än tre led som innehåller ordet ”att” kan de läsas på två sätt. Antingen så att tillsynsmyndigheten ska försöka förmå Försvarsmakten:

– att vidta åtgärder för att behandlingen ska bli författningsenlig, eller
– att fullgöra andra skyldigheter

eller så att tillsynsmyndigheten ska försöka förmå Försvarsmakten att vidta åtgärder:

– för att behandlingen ska bli författningsenlig eller
– [för] att fullgöra andra skyldigheter.

Skillnaden mellan de två alternativen är förvisso från innehållsmässig synpunkt relativt marginell, men det förhållandet att bestämmelsen kan förstås på två sätt gör den svårläst. Om syftet är att bestämmelsen ska läsas på det senare sättet (så beskrivs bestämmelsen nämligen i det första hela stycket på s. 199 i lagrådsremissen) bör ett ”för” läggas till på sätt som visas genom hakparentesen.

I paragrafens andra stycke anges att det av ett föreläggande ska framgå när åtgärderna senast ska vara genomförda och − ”om det är lämpligt” − vilka åtgärder som ska vidtas. För att stycket ska få ett rimligt innehåll måste – både eftersom åtgärder är vad som ska föreläggas enligt första stycket 2 och eftersom ett föreläggande rimligen måste ange att någon form av åtgärd ska vidtas – ”åtgärder” antas syfta på mer preciserade uppgifter om vilka specifika åtgärder som bör vidtas. Läser man sist nämnda led så att det tar sikte på åtgärder i den bredare mening som avses i första stycket 2 skulle bestämmelsen innebära att föreläggandets innehåll bör anges bara ”om det är lämpligt”, vilket naturligtvis är orimligt. Författningstexten bör utformas så att det tydligt framgår att lämplighetsvillkoret bara avser

frågan om tillsynsmyndigheten i föreläggandet bör specificera vilka konkreta åtgärder som ska vidtas.

Lagen om behandling av personuppgifter vid Försvarets radioanstalt

2 kap. 2 §

Av samma skäl som Lagrådet angett ovan beträffande 2 kap. 2 § i förslaget till lag om behandling av personuppgifter vid Försvarsmakten kan ifrågasättas om det inte bör läggas till ett stycke i paragrafen som tydliggör att de ändamål som anges i 5 och 6 §§ är särskilda bestämmelser för försvarsunderrättelseverksamheten, men att den verksamheten även omfattas av nu aktuell paragraf.

Lagrådet föreslår att det nya stycket ges följande lydelse.

För behandling av personuppgifter i utvecklingsverksamhet inom försvarsunderrättelseverksamheten finns särskilda bestämmelser i 5 och 6 §§.

2 kap. 8 §

I paragrafen regleras s.k. sekundära ändamål, dvs. under vilka förutsättningar uppgifter får behandlas för att tillgodose ändamål hos någon annan än den som är personuppgiftsansvarig. I punkt 1 anges att det får ske om det behövs i verksamhet hos den som tar emot uppgifter om informationssäkerhet. Det är högst oklart vad som avses med denna reglering. Det sägs i författningskommentaren att den avser fall då Försvarets radioanstalt utför aktiva it-kontroller eller installerar ett tekniskt detekterings- och varningssystem. Varför Försvarets radioanstalt skulle behöva behandla personuppgifter i dessa fall framgår dock inte. Inte heller framgår vad som egentligen avses med ”att någon tar emot uppgifter om informationssäkerhet”. Sannolikt avses att Försvarets radioanstalt utför någon form av säkerhetsarbete hos en annan myndighet och radioanstalten då får del av personuppgifter hos den andra myndigheten. Detta återspeglas inte i lagtexten.

I sammanhanget bör särskilt framhållas att punkten som den nu är formulerad i mycket liten grad är begränsande: om någon tar emot uppgifter om informationssäkerhet får uppgifterna behandlas hos Försvarets radioanstalt om de behövs i verksamhet hos mottagaren. Rent språkligt omfattar denna grund för behandling av person-uppgifter betydligt mer än vad som kan antas ha varit avsett.

Bestämmelsens innehåll och utformning bör övervägas i det fortsatta lagstiftningsarbetet.

2 kap. 21 §

Se Lagrådets synpunkter och förslag i fråga om 2 kap. 23 § i förslaget till lag om behandling av personuppgifter vid Försvarsmakten.

3 kap. 1 §

I paragrafen regleras för vilka ändamål som personuppgifter får göras gemensamt tillgängliga och behandlas i uppgiftssamlingar. Med uppgiftssamlingar avses enligt 1 kap. 5 § en samling med uppgifter som med hjälp av automatiserad behandling är gemensamt tillgängliga. Det är enligt andra stycket i paragrafen regeringen eller den myndighet som regeringen bestämmer som meddelar föreskrifter om vilka uppgiftssamlingar som får finnas. Gemensamt tillgängliga är således en förutsättning för att det ska bli en uppgiftssamling. Bestämmelsen förutsätter dock enligt sin lydelse att det också ska få finnas gemensamt tillgängliga uppgifter som inte är en uppgiftssamling. Det väcker frågan om vad som skiljer uppgifter som endast är gemensamt tillgängliga från uppgifter som finns i en uppgiftssamling (förutom att det senare kräver föreskrifter av regeringen eller en myndighet som regeringen bestämmer). Det bör utvecklas närmare i kommentaren vad som avses med begreppen, hur de förhåller sig till varandra och vad det får för betydelse för möjligheten att behandla uppgifter.

Se vidare vad Lagrådet anfört i anslutning till 3 kap. 2 § i förslaget till lag om behandling av personuppgifter vid Försvarsmakten.

6 kap. 5 §

Bestämmelsen motsvarar i sak 6 kap. 4 § i förslaget till lag om behandling av personuppgifter vid Försvarsmakten. Vad Lagrådet har anfört i anslutning till den paragrafen gör sig gällande också här.

Övriga lagförslag

Lagrådet lämnar förslagen utan erinran.

Försvarsdepartementet

Utdrag ur protokoll vid regeringssammanträde den 9 september 2021

Närvarande: statsminister Löfven, ordförande, och statsråden Bolund, Johansson, Baylan, Hultqvist, Andersson, Damberg, Shekarabi, Ygeman, Ekström, Eneroth, Dahlgren, Lind, Hallberg, Nordmark, Micko, Stenevi, Olsson Fridh

Föredragande: statsrådet Hultqvist

Regeringen beslutar proposition Behandling av personuppgifter vid Försvarsmakten och Försvarets radioanstalt