

EU:s dataskyddreform
– anpassningar av vissa författningar
om allmän ordning och säkerhet



SOU och Ds kan köpas från Wolters Kluwers kundservice.
Beställningsadress: Wolters Kluwers kundservice, 106 47 Stockholm
Ordertelefon: 08-598 191 90
E-post: kundservice@wolterskluwer.se
Webbplats: wolterskluwer.se/offentligapublikationer

För remissutsändningar av SOU och Ds svarar Wolters Kluwer Sverige AB
på uppdrag av Regeringskansliets förvaltningsavdelning.

Svara på remiss – hur och varför

Statsrådsberedningen, SB PM 2003:2 (reviderad 2009-05-02).

En kort handledning för dem som ska svara på remiss.

Häftet är gratis och kan laddas ner som pdf från eller beställas på regeringen.se/remisser

Omslag: Regeringskansliets standard

Tryck: Elanders Sverige AB, Stockholm 2017

ISBN 978-91-38-24705-1

ISSN 0284-6012

Till Justitiedepartementet

Den 18 oktober 2016 beslutade statsrådet Anders Ygeman att uppdra åt hovrättsrådet, tillika vice ordföranden på avdelning, Eva Lönqvist att biträda Justitiedepartementet med att undersöka vilka anpassningar som är behövliga eller lämpliga och lämna förslag på de författningsändringar som EU:s dataskyddsreform föranleder i fråga om den personuppgiftsreglering som enheten för lagstiftning om allmän ordning och säkerhet och samhällets krisberedskap vid Justitiedepartementet ansvarar för, och som inte tas om hand av Dataskyddsutredningen eller Utredningen om 2016 års dataskyddsdirektiv. Samma dag anställdes som sekreterare numera rådmannen Hedvig Burman.

Vi har under utarbetandet av denna promemoria arbetat i nära samråd och har därför valt att skriva i vi-form.

Med denna promemoria är uppdraget slutfört.

Göteborg i november 2017

Eva Lönqvist

/Hedvig Burman

Innehåll

Vissa förkortningar	11
Sammanfattning	13
1 Författningsförslag.....	17
1.1 Förslag till kustbevakningsdatalag (2018:00)	17
1.2 Förslag till kustbevakningsdataförordning (2018:00)	23
1.3 Förslag till lag om ändring i vapenlagen (1996:67)	25
1.4 Förslag till lag om ändring i lagen (1998:620) om belastningsregister	27
1.5 Förslag till lag om ändring i lagen (1998:621) om misstankeregister	30
1.6 Förslag till lag om ändring i lagen (2000:344) om Schengens informationssystem	33
1.7 Förslag till förordning om ändring i förordningen (1990:415) om införsel av farliga föremål	35
1.8 Förslag till förordning om ändring i förordningen (2000:836) om Schengens informationssystem	36
1.9 Förslag till förordning om ändring i förordningen (2008:1396) om förenklat uppgiftsutbyte mellan brottsbekämpande myndigheter i Europeiska unionen.....	37
1.10 Förslag till förordning om ändring i förordningen (2015:476) om behandling av personuppgifter i Nationellt forensiskt centrums uppdragsverksamhet	38

2	Utgångspunkter	41
2.1	Inledning	41
2.2	Kort om huvuddragen i dagens reglering av personuppgiftsbehandling.....	41
2.2.1	Regeringsformen	41
2.2.2	Personuppgiftslagen och registerförfattningar	42
2.3	EU:s dataskyddsreform.....	44
2.3.1	Tidigare EU-rättsakter.....	44
2.3.2	Reformen – två nya EU-rättsakter om personuppgiftsbehandling	45
2.3.3	Förslaget till dataskyddslag	47
2.3.4	Förslaget till brottsdatalog m.m.	48
2.3.5	Något om gränsdragningen mellan direktivet och förordningen	48
2.4	Vårt uppdrag och dess genomförande.....	49
2.5	Allmänna överväganden om anpassningen av registerförfattningar till dataskyddsförordningen.....	51
2.5.1	Dataskyddsförordningens tillämpningsområde	51
2.5.2	Rättslig grund för personuppgiftsbehandlingen	52
2.5.3	Övergripande om möjligheten att behålla och införa särreglering	56
2.5.4	Bestämmelser som är förenliga med dataskyddsförordningen	57
2.5.5	Personnummer	68
2.5.6	Känsliga personuppgifter.....	69
2.5.7	Bestämmelser som inte kan behållas	71
2.5.8	Den enskildes rättigheter.....	72
2.5.9	Behovet av nya bestämmelser.....	80
2.6	Allmänna överväganden om anpassningen av registerförfattningar till det nya dataskyddsdirektivet.....	85
2.6.1	Rättslig grund för personuppgiftsbehandlingen	85
2.6.2	Övergripande om möjligheten att införa och behålla särreglering.....	86
2.6.3	Bestämmelser som är förenliga med direktivet	87

2.6.4	Känsliga personuppgifter	93
2.6.5	Bestämmelser som inte kan behållas	93
2.6.6	Den enskildes rättigheter	94
2.6.7	Behovet av nya bestämmelser	94
3	Kustbevakningsdatalagen och -förordningen	99
3.1	Vårt uppdrag.....	99
3.2	Om författningarna	99
3.3	En ny kustbevakningsdatalag inom dataskyddsförordningens tillämpningsområde	101
3.4	Överväganden om befintliga bestämmelser	102
3.5	Överväganden om och förslag till bestämmelser i en ny kustbevakningsdatalag och -förordning	112
3.5.1	Lagens tillämpningsområde och huvudsakliga innehåll	112
3.5.2	Förhållandet till dataskyddsförordningen och dataskyddslagen	117
3.5.3	Primära och sekundära ändamål samt finalitetsprincipen	118
3.5.4	Känsliga personuppgifter	120
3.5.5	Elektroniskt utlämnande av personuppgifter	122
3.5.6	Information till den registrerade	123
3.5.7	Längsta tid för behandling	127
3.5.8	En ny kustbevakningsdataförordning	129
4	Vapenlagen, vapenförordningen och förordningen om tillstånd till införsel av vissa farliga föremål.....	131
4.1	Vapenlagen och vapenförordningen	131
4.1.1	Kort om det nya vapendirektivet.....	133
4.1.2	Vilken EU-rättsakt är tillämplig?	133
4.1.3	Överväganden om befintliga bestämmelser	135
4.1.4	Överväganden om och förslag till författningsändringar	143
4.2	Förordningen om tillstånd till införsel av vissa farliga föremål.....	146

4.2.1	Om författningen.....	146
4.2.2	Överväganden och förslag	148
5	Lagen och förordningen om belastningsregister	151
5.1	Om författningarna	151
5.2	Vilken EU-rättsakt är tillämplig?	154
5.3	Överväganden om befintliga bestämmelser i förhållande till det nya dataskyddsdirektivet.....	162
5.4	Överväganden om befintliga bestämmelser i förhållande till dataskyddsförordningen	175
5.5	Överväganden om och förslag till författningsändringar ..	182
6	Lagen och förordningen om misstankeregister.....	195
6.1	Om författningarna	195
6.2	Vilken EU-rättsakt är tillämplig?	196
6.3	Överväganden om befintliga bestämmelser i förhållande till det nya dataskyddsdirektivet.....	200
6.4	Överväganden om befintliga bestämmelser i förhållande till dataskyddsförordningen.....	207
6.5	Överväganden om och förslag till författningsändringar ..	211
7	Lagen och förordningen om Schengens informationssystem	219
7.1	Om författningarna	219
7.2	Vilken EU-rättsakt är tillämplig?	222
7.3	Överväganden om befintliga bestämmelser	224
7.3.1	Överväganden i förhållande till det nya dataskyddsdirektivet	224
7.3.2	Överväganden i förhållande till dataskyddsförordningen	228
7.3.3	Genomförandet av rådsbeslutet när personuppgiftslagen upphävs	232

7.4	Överväganden om och förslag till författningsändringar ...	237
8	Förordningen om förenklat uppgiftsutbyte mellan brottsbekämpande myndigheter i Europeiska unionen .	243
8.1	Om författningen.....	243
8.2	Överväganden och förslag	245
9	Förordningen om behandling av personuppgifter i Nationellt forensiskt centrums uppdragsverksamhet	247
9.1	Om författningen.....	247
9.2	Överväganden och förslag	249
10	Lagen om hotell- och pensionatrörelse	255
10.1	Om författningen.....	255
10.2	Överväganden	257
11	Förordningen om tjänstekort	261
11.1	Om författningen.....	261
11.2	Överväganden	261
12	Förordningen om utdrag ur folkbokföringsdatabasen i och för utredning angående brott m.m.	265
12.1	Om författningen.....	265
12.2	Överväganden	265
13	Efterlysningskungörelsen	269
13.1	Om författningen.....	269
13.2	Överväganden	271
14	Ikraftträdande och övergångsbestämmelser	277
14.1	Författningsförslag inom dataskyddsförordningens tillämpningsområde	277

14.2	Författningsförslag inom det nya dataskyddsdirektivets tillämpningsområde	278
14.3	Författningsförslag inom både det nya dataskyddsdirektivets och dataskyddsförordningens tillämpningsområde	279
15	Konsekvenser	281
16	Författningskommentar	285
16.1	Förslaget till kustbevakningsdatalag	285
16.2	Förslaget till lag om ändring i vapenlagen.....	293
16.3	Förslaget till lag om ändring i lagen om belastningsregister	294
16.4	Förslaget till lag om ändring i lagen om misstankeregister	298
16.5	Förslaget till lag om ändring i lagen om Schengens informationssystem.....	299
Bilaga 1	Uppdraget.....	301

Vissa förkortningar

1995 års dataskyddsdirektiv	Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter
det nya dataskyddsdirektivet	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
dataskyddsförordningen	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)

brottsdatalagen

förslag till brottsdatalag
(2018:00), SOU 2017:29

dataskyddslagen

förslag till lag (2018:00) med
kompletterande bestämmelser till
EU:s dataskyddsförordning,
SOU 2017:39

Sammanfattning

Bakgrund

Inom EU har det antagits en ny reglering av skyddet för enskilda vid behandling av personuppgifter. Den består av två rättsliga instrument, en förordning och ett direktiv.

Dataskyddsförordningen utgör en ny generell reglering för behandling av personuppgifter inom EU. Dataskyddsförordningen är direkt tillämplig i medlemsstaterna. En följd av att förordningen ska tillämpas direkt är att personuppgiftslagen (1998:204) måste upphävas. Samtidigt både förutsätter och möjliggör dataskyddsförordningen kompletterande nationella bestämmelser av olika slag.

Dataskyddsförordningen ska inte tillämpas på personuppgiftsbehandling som utförs av behöriga myndigheter för att bl.a. bekämpa och lagföra brott. På detta område gäller istället det nya dataskyddsdirektivet, som, till skillnad från förordningen, ska genomföras i medlemsstaternas nationella rätt.

Dataskyddsutredningen har haft i uppdrag att föreslå de anpassningar och kompletterande författningsbestämmelser på generell nivå som dataskyddsförordningen ger anledning till. Utredningen har lämnat förslag till en ny lag, dataskyddslagen. Utredningen om 2016 års dataskyddsdirektiv har haft det huvudsakliga uppdraget att genomföra det nya dataskyddsdirektivet i svensk rätt. Utredningen har lämnat förslag till en ny ramlag inom direktivets tillämpningsområde, brottsdatalagen. Utredningen har också lämnat förslag på anpassningar av flera s.k. registerförfattningar, som tillämpas av olika brottsbekämpande myndigheter, exempelvis Polismyndigheten.

Vårt uppdrag

Vårt uppdrag har varit att se över och överväga vilka anpassningar som kan behövas i vissa registerförfattningar som Enheten för lagstiftning om allmän ordning och säkerhet och samhällets krisberedskap vid Justitiedepartementet (Enheten) ansvarar för. Flera av registerförfattningarna inom Enhetens ansvarsområde har ingått i det uppdrag som Utredningen om 2016 års dataskyddsdirektiv har haft. Vårt uppdrag har rört de flesta andra författningar inom Enhetens ansvarsområde som i någon mån reglerar frågor om personuppgiftsbehandling. Vårt uppdrag har bl.a. gällt kustbevakningsdatalagen, lagen och förordningen om belastningsregister, lagen och förordningen om Schengens informationssystem och vapenlagen.

Flera av de registerförfattningar som ingått i vårt utredningsuppdrag reglerar personuppgiftsbehandling inom både det nya dataskyddsdirektivets och dataskyddsförordningens tillämpningsområde.

Våra överväganden och förslag

En av våra utgångspunkter har varit att gällande svensk rätt bör förändras så lite som möjligt till följd av EU:s dataskyddsreform. De väsentliga avvägningarna avseende behovet av författningsreglering och skyddet för den personliga integriteten är redan gjorda.

Vi har kommit fram till att författningsregleringen i huvudsak är förenlig både med genomförandet av det nya dataskyddsdirektivet och med dataskyddsförordningen.

När det gäller författningsregleringen av Kustbevakningens personuppgiftsbehandling har vårt uppdrag gällt endast den del av kustbevakningsdatalagen som omfattas av dataskyddsförordningens tillämpningsområde. Vi föreslår, efter samråd med Utredningen om 2016 års dataskyddsdirektiv, att denna del av Kustbevakningens personuppgiftsbehandling ska regleras i en egen lag, som vi föreslår ska heta som den nu gällande lagen – kustbevakningsdatalagen. Den personuppgiftsbehandling som sker inom Kustbevakningens brottsbekämpande och lagförande verksamhet kommer enligt förslag från Utredningen om 2016 års dataskyddsdirektiv att regleras i den nu gällande lagen, som får ett till viss del

nytt innehåll och föreslås byta namn till Kustbevakningens brottsdatalog.

Våra författningsförslag i övrigt syftar i stort sett till att klargöra förhållandet mellan de aktuella registerförfattningarna och de nya generella regelverken avseende personuppgiftsbehandling (dvs. dataskyddsförordningen jämte dataskyddslagen och/eller brottsdatalogen). I övrigt föreslår vi tillägg och ändringar för att anpassa registerförfattningarna, bl.a. genom att utmönstra hänvisningar till personuppgiftslagen.

Konsekvenser

Våra förslag är i huvudsak av lagteknisk karaktär. Vi bedömer att de i sig inte kommer att föra med sig annat än i sammanhanget marginella kostnader för de berörda myndigheterna.

Dataskyddsreformens övergripande syfte är att förstärka skyddet för den personliga integriteten vid behandling av personuppgifter. De effekter som kan uppnås på detta område menar vi i första hand följer av de nya generella regelverken och inte av våra förslag.

Ikraftträdande

Dataskyddsförordningen ska börja tillämpas den 25 maj 2018 och vi föreslår att författningsändringar som berörs endast av förordningen träder i kraft samma datum. Författningsändringar som är beroende av brottsdatalogens ikraftträdande föreslår vi ska träda i kraft samma dag som den lagen, den 1 maj 2018.

1 Författningsförslag

1.1 Förslag till kustbevakningsdatalag (2018:00)

Härigenom föreskrivs följande.

Lagens syfte

1 § Syftet med denna lag är att ge Kustbevakningen möjlighet att behandla personuppgifter på ett ändamålsenligt sätt i sin operativa verksamhet och att skydda människor mot att deras personliga integritet kränks vid sådan behandling.

Lagens tillämpningsområde

2 § Denna lag gäller vid behandling av personuppgifter i Kustbevakningens operativa verksamhet som rör:

1. sjöövervakning,
2. räddningstjänst,
3. samordning av civila behov av sjöövervakning och förmedling av civil sjöinformation, och
4. internationellt samarbete.

Lagen gäller inte vid behandling av personuppgifter som omfattas av Kustbevakningens brottsdatalag (2018:00).

Lagen gäller endast om behandlingen är helt eller delvis automatiserad eller om personuppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

Förhållandet till annan reglering av personuppgiftsbehandling

3 § Denna lag innehåller bestämmelser som kompletterar 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).

4 § Även lagen (2018:00) med kompletterande bestämmelser till EU:s dataskyddsförordning gäller vid behandling av personuppgifter enligt denna lag, om inte annat följer av denna lag eller föreskrifter som meddelats i anslutning till den.

Lagens tillämpning på juridiska personer

5 § Följande bestämmelser om personuppgifter gäller även vid behandling av uppgifter om juridiska personer:

1. 6 § om personuppgiftsansvar,
2. 7–11 §§ om ändamålen för behandlingen,
3. 16 § om tillgången till personuppgifter och
4. 25 § om bevarande och gallring.

Personuppgiftsansvar

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

Ändamål för behandling

7 § Personuppgifter får behandlas om det behövs för att

1. bedriva sjöövervakning för att övervaka den allmänna ordningen och säkerheten till sjöss samt bedriva den kontroll och tillsyn som Kustbevakningen är skyldig att utföra,
2. bedriva räddningstjänst,
3. samordna civila behov av sjöövervakning och förmedla civil sjöinformation till berörda myndigheter,

4. utreda och besluta i ärenden om vattenföreningssavgift samt ta emot sådana avgifter, eller

5. fullgöra skyldigheter inom ramen för internationellt samarbete med sjöövervakning och räddningstjänst.

8 § Utöver vad som anges i 7 § får personuppgifter behandlas om

1. behandlingen är nödvändig för diarieföring, eller

2. uppgifterna har lämnats i en anmälan eller liknande och behandlingen är nödvändig för handläggningen.

9 § Personuppgifter som behandlas enligt 7 § får även behandlas om det är nödvändigt för att tillhandahålla information som behövs i

1. Kustbevakningens brottsbekämpande och lagförande verksamhet och verksamhet för att upprätthålla allmän ordning och säkerhet,

2. en annan myndighets verksamhet

a. om Kustbevakningen enligt lag eller förordning är skyldig att bistå myndigheten med viss uppgift, eller

b. om informationen tillhandahålls inom ramen för myndighetsöverskridande samverkan, och

3. likartad verksamhet hos en utländsk myndighet.

10 § Personuppgifter som behandlas enligt 7 § får även behandlas om det är nödvändigt för att tillhandahålla information till riksdagen och regeringen samt, i den utsträckning skyldighet att lämna uppgifter följer av lag eller förordning, till annan.

11 § I ett enskilt fall får personuppgifter som behandlas enligt 7 § även behandlas för att tillhandahålla information för något annat ändamål än de som anges i 9 och 10 §§ under de förutsättningar som framgår av artikel 5.1 b och 6.4 a–e i Europaparlamentets och rådets förordning (EU) 2016/679.

Behandling av känsliga personuppgifter

12 § Sådana särskilda kategorier av personuppgifter som anges i artikel 9.1 i Europaparlamentets och rådets förordning (EU) 2016/679 (känsliga personuppgifter) får inte behandlas.

Om uppgifter om en person behandlas får de, utan hinder av det som sägs i första stycket, kompletteras med känsliga personuppgifter när det är absolut nödvändigt för ändamålet med behandlingen. Känsliga personuppgifter får också behandlas med stöd av 8 §.

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

13 § Det är förbjudet att utföra sökningar i syfte att få fram ett personurval grundat på känsliga personuppgifter.

Första stycket hindrar inte att uppgifter som beskriver en persons utseende används som sökbegrepp.

Tillgången till personuppgifter

14 § Med gemensamt tillgängliga uppgifter avses i denna lag personuppgifter som görs eller har gjorts gemensamt tillgängliga i Kustbevakningens operativa verksamhet och som fler än endast ett fåtal personer inom myndigheten har rätt att ta del av.

15 § Personuppgifter som får behandlas enligt 7 § får göras gemensamt tillgängliga.

16 § Tillgången till personuppgifter ska alltid begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela närmare föreskrifter om tillgången till personuppgifter.

Utlämnande av personuppgifter

17 § Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om i vilken utsträckning personuppgifter får lämnas ut till svenska och utländska myndigheter.

Bestämmelser om att uppgifter får lämnas ut finns även i offentlighets- och sekretesslagen (2009:400).

18 § Utlämnande genom direktåtkomst är tillåtet bara i den utsträckning som följer av denna lag. Bestämmelser om direktåtkomst finns i 20–23 §§.

19 § 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 begränsningar av möjligheterna att lämna ut personuppgifter elektroniskt.

Direktåtkomst

20 § Direktåtkomst får endast avse personuppgifter som har gjorts gemensamt tillgängliga. Direktåtkomsten får inte avse personuppgifter som anges i 12 § första stycket.

21 § Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om vilka svenska myndigheter som får ha direktåtkomst till personuppgifter som behandlas med stöd av 7 § och om utländska myndigheter får ha sådan åtkomst.

22 § En myndighet som medgetts direktåtkomst ansvarar för att tillgången till personuppgifter begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter.

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

Information till den registrerade

24 § Information enligt artikel 13 i Europaparlamentets och rådets förordning (EU) 2016/679 behöver inte lämnas vid behandling som består av insamling av personuppgifter genom bilder eller ljud, om inte behandlingen i övrigt innebär en direkt identifiering av en person. Sådan information behöver inte heller lämnas om uppgifterna samlas in i samband med larm och det med hänsyn till omständigheterna inte finns tid att lämna informationen.

Bevarande och gallring

25 § Personuppgifter som behandlas automatiserat ska gallras så snart uppgifterna inte längre behövs för det ändamål för vilket de behandlas, om inte regeringen eller den myndighet som regeringen bestämmer har meddelat föreskrifter om att gallring ska ske senast vid en viss tidpunkt eller att uppgifter får bevaras för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål.

Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om digital arkivering.

Denna lag träder i kraft den 25 maj 2018.

1.2 Förslag till kustbevakningsdataförordning (2018:00)

Härigenom föreskrivs följande.

1 § I denna förordning finns kompletterande föreskrifter om sådan behandling av personuppgifter som omfattas av kustbevakningsdatalagen (2018:00). De uttryck som används i denna förordning har samma innebörd och tillämpningsområde som i lagen.

Tillgången till personuppgifter

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

Direktåtkomst

3 § Polismyndigheten, Tullverket, Havs- och vattenmyndigheten, Naturvårdsverket, Sveriges meteorologiska och hydrologiska institut, Sjöfartsverket, Transportstyrelsen, Sveriges geologiska undersökning, Myndigheten för samhällsskydd och beredskap och Försvarsmakten får medges direktåtkomst till personuppgifter som Kustbevakningen behandlar för att samordna civila behov av sjöövervakning och för att förmedla civil sjöinformation till berörda myndigheter. Om Kustbevakningen medger direktåtkomst gäller det som anges i 20 och 22 §§ kustbevakningsdatalagen (2018:000).

4 § Kustbevakningen får meddela närmare föreskrifter om vad som krävs i fråga om behörighet och säkerhet för att myndigheten ska kunna medge direktåtkomst till personuppgifter för de myndigheter som anges i 3 § denna förordning.

Direktåtkomst till uppgifterna får inte medges innan Kustbevakningen har försäkrat sig om att den mottagande myndigheten uppfyller kraven på behörighet och säkerhet.

Gallring och bevarande

5 § Riksarkivet får, efter samråd med Kustbevakningen, meddela föreskrifter om att uppgifter som ska gallras enligt 25 § kustbevakningsdatalagen (2018:00) får bevaras för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål.

Samråd med Datainspektionen

6 § Innan Kustbevakningen meddelar föreskrifter med stöd av denna förordning, ska samråd ske med Datainspektionen i frågor som berör särskilda risker för intrång i den personliga integriteten.

Denna förordning träder i kraft den 25 maj 2018.

1.3 Förslag till lag om ändring i vapenlagen (1996:67)

Härigenom föreskrivs i fråga om vapenlagen (1996:67)¹

dels att 1 a kap. 2, 4 och 6 §§ ska upphöra att gälla,

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

dels att rubriken närmast framför 1 a kap. 1 § ska lyda ”Personuppgiftsansvar och förhållande till annan reglering av personuppgiftsbehandling”,

dels att det ska införas två nya paragrafer, 1 a kap. 2 och 4 §§, med följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

2 §

Detta kapitel innehåller bestämmelser som kompletterar 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).

Även lagen (2018:00) med kompletterande bestämmelser till EU:s dataskyddsförordning gäller vid behandling av personuppgifter enligt detta kapitel, om inte annat följer av detta kapitel eller föreskrifter som meddelats i anslutning till det.

¹ Senaste lydelse av

2 § 2014:591

4 § 2014:591

6 § 2014:591

rubriken närmast före 1 a kap. 1 § 2014:591

3 §²

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

Om uppgifter om en person behandlas *på annan grund*, får de kompletteras med sådana uppgifter som avses i första stycket när det är absolut nödvändigt för *syftet* med behandlingen. Uppgifter som avses i första stycket får också behandlas om det är nödvändigt för diarieföring eller om uppgifterna har lämnats till Polismyndigheten i en anmälan eller liknande och behandlingen är nödvändig för handläggningen.

Sådana särskilda kategorier av personuppgifter som anges i artikel 9.1 i Europaparlamentets och rådets förordning (EU) 2016/679 (känsliga personuppgifter) får inte behandlas.

Om uppgifter om en person behandlas får de kompletteras med sådana uppgifter som avses i första stycket när det är absolut nödvändigt för *ändamålet* med behandlingen. Uppgifter som avses i första stycket får också behandlas om det är nödvändigt för diarieföring eller om uppgifterna har lämnats till Polismyndigheten i en anmälan eller liknande och behandlingen är nödvändig för handläggningen.

4 §

Det är förbjudet att utföra sökningar i syfte att få fram ett personurval grundat på känsliga personuppgifter.

Denna lag träder i kraft den 25 maj 2018.

² Senaste lydelse 2014:591.

1.4 Förslag till lag om ändring i lagen (1998:620) om belastningsregister

Härigenom föreskrivs i fråga om lagen (1998:620) om belastningsregister³

dels att 1 b § ska upphöra att gälla,

dels att 1 a, 2, 9 och 20 §§ och rubriken närmast före 20 § ska ha följande lydelse,

dels att det ska införas en ny paragraf, 1 b §, med följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

1 a §⁴

Denna lag gäller utöver *personuppgiftslagen (1998:204)*

Denna lag gäller utöver *brottsdatalagen (2018:00)*.

Sökförbudet i 2 kap. 14 § brottsdatalagen (2018:000) hindrar inte att uppgifter om brottsrubriceringar och om verkställighet av påföljd används vid sökning i belastningsregistret.

1 b §

För behandling av personuppgifter enligt denna lag för ändamål utanför brottsdatalagens (2018:00) tillämpningsområde finns bestämmelser om behandling av personuppgifter i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om

³ Senaste lydelse av 1 b § 2013:331.

⁴ Senaste lydelse 2013:331.

upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) och i lagen (2018:00) med kompletterande bestämmelser till EU:s dataskyddsförordning.

2 §⁵

Belastningsregistret ska föras för att ge information om sådana belastningsuppgifter som behövs i verksamhet hos

1. Polismyndigheten, Säkerhetspolisen, Skatteverket, Tullverket och Kustbevakningen för att förebygga, upptäcka och utreda brott,

2. åklagarmyndigheter för beslut om förundersökning och åtal samt för utfärdande av strafföreläggande,

3. allmänna domstolar för straffmätning och val av påföljd och

4. Polismyndigheten och andra myndigheter vid sådan lämplighetsprövning, tillståndsprövning eller annan prövning som anges i författning.

Registret får användas också för att till en enskild lämna uppgifter som är av särskild betydelse i hans eller hennes verksamhet.

9 §⁶

En enskild har rätt att på begäran skriftligen få ta del av samtliga uppgifter ur registret om sig själv. Sådana uppgifter ska på begäran lämnas ut utan avgift en gång per kalenderår.

En enskild som behöver ett registerutdrag om sig själv har rätt att få ett begränsat utdrag ur registret

1. för att kunna ta till vara sin rätt i ett främmande land eller få tillstånd att resa in, bosätta sig eller arbeta där,

En enskilds rätt att på begäran få information om behandling av personuppgifter följer av 4 kap. 3 § brottsdatalagen.

En enskild som behöver ett registerutdrag om sig själv har rätt att *därutöver* få ett begränsat utdrag ur registret

⁵ Senaste lydelse 2014:593.

⁶ Senaste lydelse 2015:987.

2. enligt bestämmelser i skollagen (2010:800),
3. enligt bestämmelser i lagen (2005:405) om försäkringsförmedling,
4. enligt bestämmelser i lagen (2007:171) om registerkontroll av personal vid vissa boenden som tar emot barn,
5. enligt bestämmelser i lagen (2010:479) om registerkontroll av personal som utför vissa insatser åt barn med funktionshinder, eller
6. enligt bestämmelser i lagen (2013:852) om registerkontroll av personer som ska arbeta med barn.

Regeringen, eller i fråga om andra stycket punkterna 1–3 den myndighet regeringen bestämmer, får meddela föreskrifter om vilka uppgifter ett sådant utdrag ska innehålla.

En begäran om uppgifter ur registret ska vara skriftlig *och undertecknad av den sökande.*

En begäran om uppgifter ur registret ska vara skriftlig. *Polismyndigheten ska säkerställa att begäran görs av en behörig person.*

Rättelse och skadestånd

Skadestånd för personuppgiftsbehandling inom brottsdatalogens tillämpningsområde

20 §

Bestämmelserna i personuppgiftslagen (1998:204) om rättelse och skadestånd gäller vid behandling av personuppgifter enligt denna lag eller enligt föreskrifter som har meddelats med stöd av lagen.

Bestämmelsen i 7 kap. 1 § brottsdatalogen (2018:00) om skadestånd tillämpas på motsvarande sätt vid behandling av personuppgifter enligt denna lag eller enligt föreskrifter som har meddelats med stöd av lagen och som omfattas av brottsdatalogens tillämpningsområde.

1. Denna lag träder i kraft den 25 maj 2018 i fråga om införandet av 1 b § och i övrigt den 1 maj 2018.

2. Lagen om belastningsregister i dess lydelse före den 1 maj 2018 och personuppgiftslagen (1998:204) gäller till och med den 24 maj 2018 för sådan behandling av personuppgifter som inte omfattas av brottsdatalogens tillämpningsområde.

1.5 Förslag till lag om ändring i lagen (1998:621) om misstankeregister

Härigenom föreskrivs i fråga om lagen (1998:621) om misstankeregister⁷

dels att 1 b § ska upphöra att gälla,

dels att 1 a, 2, 8 a och 15 §§ och rubriken närmast före 15 § ska ha följande lydelse,

dels att det ska införas en ny paragraf, 1 b §, med följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

Denna lag gäller utöver
personuppgiftslagen (1998:204)

1 a §⁸

Denna lag gäller utöver
brottsdatalagen (2018:00).

Sökförbudet i 2 kap. 14 § brottsdatalagen (2018:000) hindrar inte att uppgifter om brottsrubriceringar används vid sökning i misstankeregistret.

1 b §

För behandling av personuppgifter enligt denna lag för ändamål utanför brottsdatalagens (2018:00) tillämpningsområde finns bestämmelser om behandling av personuppgifter i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om

⁷ Senaste lydelse av 1 b § 2013:332.

⁸ Senaste lydelse 2013:332.

*upphävande av direktiv 95/46/EG
(allmän dataskyddsförordning)
och i lagen (2018:00) med
kompletterande bestämmelser till
EU:s dataskyddsförordning.*

2 §⁹

Misstankeregistret ska föras för att underlätta tillgången till sådana uppgifter om skäligen misstanke om brott som behövs i verksamhet hos

1. Polismyndigheten, Säkerhetspolisen, Skatteverket, Tullverket och Kustbevakningen för att förebygga, upptäcka och utreda brott,

1. Polismyndigheten, Säkerhetspolisen, Skatteverket, Tullverket och Kustbevakningen för att förebygga, *förhindra eller upptäcka brottslig verksamhet* och utreda brott,

2. åklagarmyndigheter för beslut om förundersökning och åtal och,

3. Polismyndigheten och andra myndigheter vid sådan lämplighetsprövning, tillståndsprövning eller annan prövning som anges i författning.

Registret får användas också för att till en enskild lämna uppgifter som är av särskild betydelse i hans eller hennes verksamhet.

8 a §¹⁰

En enskild som behöver ett registerutdrag om sig själv enligt bestämmelser i lagen (2007:171) om registerkontroll av personal vid vissa boenden som tar emot barn har rätt att få ett begränsat utdrag ur registret. Regeringen får meddela föreskrifter om vilka uppgifter ett sådant utdrag ska innehålla.

⁹ Senaste lydelse 2014:594.

¹⁰ Senaste lydelse 2015:988.

En begäran om uppgifter ur registret ska vara skriftlig *och undertecknad av den sökande.*

En begäran om uppgifter ur registret ska vara skriftlig. *Polismyndigheten ska säkerställa att begäran görs av en behörig person.*

Rättelse och skadestånd

Skadestånd för personuppgiftsbehandling inom brottsdatalogens tillämpningsområde

Bestämmelserna i personuppgiftslagen (1998:204) om rättelse och skadestånd gäller vid behandling av personuppgifter enligt denna lag eller enligt föreskrifter som har meddelats med stöd av lagen.

15 §

Bestämmelsen i 7 kap. 1 § brottsdatalogen (2018:00) om skadestånd tillämpas på motsvarande sätt vid behandling av personuppgifter enligt denna lag eller enligt föreskrifter som har meddelats med stöd av lagen och som omfattas av brottsdatalogens tillämpningsområde.

1. Denna lag träder i kraft den 25 maj 2018 i fråga om införandet av 1 b § och i övrigt den 1 maj 2018.

2. Lagen om misstankeregister i dess lydelse före den 1 maj 2018 och personuppgiftslagen (1998:204) gäller till och med den 24 maj 2018 för sådan behandling av personuppgifter som inte omfattas av brottsdatalogens tillämpningsområde.

1.6 Förslag till lag om ändring i lagen (2000:344) om Schengens informationssystem

Härigenom föreskrivs i fråga om lagen (2000:344) om Schengens informationssystem¹¹

dels att 15 och 17 §§ ska upphöra att gälla,

dels att 16 § ska ha följande lydelse,

dels att rubriken närmast före 7 § ska lyda ”Förbud mot registrering av vissa uppgifter”,

dels att det ska införas två nya paragrafer, 1 a och 1 b §§ och närmast före 1 a § en ny rubrik, med följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

*Förhållande till annan reglering
av personuppgiftsbehandling*

1 a §

Denna lag gäller utöver brottsdatalagen (2018:00).

Bestämmelserna i 7, 10 och 13 §§ tillämpas istället för 2 kap. 4, 11 och 22 §§ och 8 kap. brottsdatalagen.

1 b §

För behandling av personuppgifter enligt denna lag för ändamål utanför brottsdatalagens (2018:00) tillämpningsområde finns bestämmelser om behandling av personuppgifter i Europaparlamentets och rådets förordning (EU) 2016/679 av den

¹¹ Senaste lydelse av

15 § 2014:595

17 § 2014:595

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 data-skyddsförordning) och i lagen (2018:00) med kompletterande bestämmelser till EU:s data-skyddsförordning.

Bestämmelserna i 4 § första stycket 3 och 7 § tillämpas istället för 3 kap. 3 § lagen (2018:00) med kompletterande bestämmelser till EU:s dataskyddsförordning.

16 §¹²

Vid behandling av personuppgifter enligt denna lag eller enligt föreskrifter som har meddelats med stöd av lagen gäller i fråga om skadestånd 48 § första stycket personuppgiftslagen (1998:204).

Vid behandling av personuppgifter enligt denna lag eller enligt föreskrifter som har meddelats med stöd av lagen och som omfattas av brottsdatalagens tillämpningsområde gäller i fråga om skadestånd 7 kap. 1 § brottsdatalagen (2018:00).

1. Denna lag träder i kraft den 25 maj 2018 i fråga om införandet av 1 b § och i övrigt den 1 maj 2018.

2. Lagen om Schengens informationssystem i dess lydelse före den 1 maj 2018 och personuppgiftslagen (1998:204) gäller till och med den 24 maj 2018 för sådan behandling av personuppgifter som inte omfattas av brottsdatalagens tillämpningsområde.

¹² Senaste lydelse 2010:380.

1.7 Förslag till förordning om ändring i förordningen (1990:415) om införsel av farliga föremål

Härigenom föreskrivs i fråga om förordningen (1990:415) om införsel av farliga föremål att 4 § ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

4 §¹³

I fråga om föremål som omfattas av denna förordning ska i tillämpliga delar det gälla som föreskrivs om skjutvapen i 1 kap. 8 §, 1 a kap. 7 §, 2 kap. 11 §, 12 § andra meningen, 14 och 15 §§, 10 kap. 1 och 2 §§ samt 11 kap. 2 § f vapenlagen (1996:67) och 2 kap. 2 § första stycket 1, 6 och 11 §§, 3 kap. 1 § första stycket och 2 § samt 4 kap. 4 § vapenförordningen (1996:70).

I fråga om föremål som omfattas av denna förordning ska i tillämpliga delar det gälla som föreskrivs om skjutvapen i 1 kap. 8 §, 1 a kap. 2, 7 och 8 §§, 2 kap. 11 §, 12 § andra meningen, 14 och 15 §§, 10 kap. 1 och 2 §§ samt 11 kap. 2 § f vapenlagen (1996:67) och 2 kap. 2 § första stycket 1, 6 och 11 §§, 3 kap. 1 § första stycket och 2 § samt 4 kap. 4 § vapenförordningen (1996:70).

Denna förordning träder i kraft den 25 maj 2018.

¹³ Senaste lydelse 2017:505.

1.8 Förslag till förordning om ändring i förordningen (2000:836) om Schengens informationssystem

Härigenom föreskrivs i fråga om förordningen (2000:836) om Schengens informationssystem att 21 och 22 §§ ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

21 §¹⁴

I 25–27 §§ personuppgiftslagen (1998:204) finns bestämmelser om information till den som har registrerats.

Information enligt 26 § personuppgiftslagen ska lämnas inom en månad eller, om det finns särskilda skäl, senast två månader efter det att ansökan gjordes.

Information om personuppgiftsbehandling på begäran av den registrerade ska lämnas inom en månad eller, om det finns särskilda skäl, senast två månader efter det att ansökan gjordes.

22 §¹⁵

En person som har ansökt om rättelse eller annan åtgärd enligt 15 § lagen (2000:344) om Schengens informationssystem ska senast tre månader efter det att ansökan gjordes informeras om de åtgärder som har vidtagits.

En person som har ansökt om rättelse eller annan åtgärd avseende personuppgiftsbehandling som en registrerad har rätt att begära ska senast tre månader efter det att ansökan gjordes informeras om de åtgärder som har vidtagits.

Denna förordning träder i kraft den 1 maj 2018.

¹⁴ Senaste lydelse 2013:131. Ändringen innebär bl.a. att första stycket tas bort.

¹⁵ Senaste lydelse 2013:131.

1.9 Förslag till förordning om ändring i förordningen (2008:1396) om förenklat uppgiftsutbyte mellan brottsbekämpande myndigheter i Europeiska unionen

Härigenom föreskriv i fråga om förordningen (2008:1396) om förenklat uppgiftsutbyte mellan brottsbekämpande myndigheter i Europeiska unionen¹⁶ att 1 a § ska upphöra att gälla vid utgången av april 2018.

¹⁶ Senaste lydelse av 1 a § 2013:348.

1.10 Förslag till förordning om ändring i förordningen (2015:476) om behandling av personuppgifter i Nationellt forensiskt centrum uppdragsverksamhet

Härigenom föreskrivs i fråga om förordning (2015:476) om behandling av personuppgifter i Nationellt forensiskt centrum uppdragsverksamhet

dels att 2 och 6 §§ ska upphöra att gälla,

dels att det ska införas en ny paragraf, 2 §, av följande lydelse,

dels att 1 § och rubriken närmast före 2 § ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

1 §

Denna förordning gäller vid helt eller delvis automatiserad behandling av personuppgifter vid undersökningar som Nationellt forensiskt centrum i Polismyndigheten utför på uppdrag av andra än de myndigheter eller organ som anges i 5 kap. 1 § polisdatalagen (2010:361).

Denna förordning gäller vid helt eller delvis automatiserad behandling av personuppgifter vid undersökningar som Nationellt forensiskt centrum i Polismyndigheten utför på uppdrag av andra än de myndigheter eller organ som anges i 6 kap. 1 § polisens brottsdatalag (2010:361).

Förhållande till personuppgiftslagen

Förhållande till annan reglering av personuppgiftsbehandling

2 §

Denna förordning innehåller bestämmelser som kompletterar 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).

Även lagen (2018:00) med kompletterande bestämmelser till EU:s dataskyddsförordning gäller vid behandling av personuppgifter enligt denna förordning om inte annat följer av denna förordning.

Denna förordning träder i kraft den 1 maj 2018 ifråga om 1 § och i övrigt den 25 maj 2018.

2 Utgångspunkter

2.1 Inledning

Det här kapitlet inleds med en kortfattad beskrivning av huvuddragen i dagens reglering av personuppgiftsbehandling. Därefter (avsnitt 2.3) redogör vi kort för EU:s dataskyddsreform och för två centrala svenska utredningar som har lagt fram förslag och överväganden under vår utredningstid. Vårt uppdrag presenteras i avsnitt 2.4. I de två sista avsnitten i kapitlet gör vi allmänna överväganden om anpassningen av svenska författningar till de två EU-rättsakterna som ingår i EU:s dataskyddsreform – dataskyddsförordningen och det nya dataskyddsdirektivet. Vi har valt att göra så eftersom flera av de registerförfattningar som vi ska analysera inom ramen för vårt uppdrag innehåller likartade bestämmelser. Samma ändringar och tillägg aktualiseras också i flera lagar. I de följande kapitlen i promemorian överväger vi sedan varje författning för sig och överväger och motiverar ytterligare de förslag till författningsändringar som vi ansett vara behövliga och lämpliga.

2.2 Kort om huvuddragen i dagens reglering av personuppgiftsbehandling

2.2.1 Regeringsformen

Enligt 2 kap. 6 § andra stycket regeringsformen är var och en – utöver vad som anges i första stycket i paragrafen – 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. Skyddet mot intrång får endast begränsas i lag och under förutsättning bl.a. att begränsningen sker för att tillgodose ändamål

som är godtagbara i ett demokratiskt samhälle och inte går utöver vad som är nödvändigt med hänsyn till de ändamål som har föranlett den (2 kap. 20 och 21 §§ regeringsformen).

Automatiserad behandling av personuppgifter, i registerform eller i andra informationshanteringssystem, kan innebära en kartläggning av enskildas förhållanden, även om syftet med behandlingen är ett annat.¹ Grundlagsskyddet omfattar dock bara betydande intrång i den personliga integriteten. Vid bedömningen av vad som kan anses vara ett betydande intrång när det gäller personuppgiftsbehandling ska vägas in uppgifternas karaktär och omfattning samt ändamålet med behandlingen.²

Det nuvarande skyddet mot betydande intrång i den personliga integriteten i 2 kap. 6 § regeringsformen trädde i kraft 2011. Även före bestämmelsens införande var det en uttalad målsättning att myndighetsregister med ett stort antal registrerade och särskilt känsligt innehåll skulle vara reglerat i lag.³

2.2.2 Personuppgiftslagen och registerförfattningar

Det är i första hand personuppgiftslagen (1998:204) som ska tillgodose regeringsformens krav på integritetsskydd när det gäller automatiserad personuppgiftsbehandling.⁴ Personuppgiftslagen genomför Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (1995 års dataskyddsdirektiv) i svensk rätt. Lagen har dock ett vidare tillämpningsområde än direktivet, bl.a. eftersom den omfattar även områden som faller utanför unionsrätten och inte gör något generellt undantag för personuppgiftsbehandling på straffrättens område (jfr artikel 3 i 1995 års dataskyddsdirektiv).

Personuppgiftslagen innehåller alltså de grundläggande bestämmelserna om personuppgiftsbehandling. Det är bestämmelser om under vilka förutsättningar personuppgiftsbehandling alls är tillåten och vilka grundläggande krav som gäller för all personuppgifts-

¹ Prop. 2009/10:80 s. 180.

² A. prop. s. 183.

³ Bl.a. bet. 1990/91:KU s. 11 och 1997/98:KU18 s. 43.

⁴ Jfr prop. 2009/10:85 s. 67.

behandling, exempelvis att personuppgifter alltid ska behandlas lagligt och korrekt och att personuppgifter ska samlas in och behandlas bara för särskilda, uttryckligt angivna och berättigade ändamål. Lagen innehåller vidare bestämmelser om den enskildes rätt till information om personuppgiftsbehandling och den enskildes tillgång till rättsmedel. Den reglerar också frågor om tillsyn och sanktioner. Vidare innehåller lagen bestämmelser avseende vissa särskilda kategorier av personuppgifter (s.k. känsliga personuppgifter, uppgifter om brott och personnummer) samt bestämmelser om vissa särskilda behandlingssituationer (automatiserade beslut och överföringar av personuppgifter till tredje land).

Personuppgiftslagen är subsidiär till andra författningar, dvs. avvikande bestämmelser i annan författning gäller framför lagen (2 §). I förarbetena anfördes att genom att det krävs en särskild författning för att avvika från det integritetsskydd som personuppgiftslagen ger, garanteras att behovet av särregler alltid övervägs nog i den ordning som gäller för författningssgivning.⁵ Det anfördes vidare att det fanns ett behov av att se över befintliga författningar och behovet av särreglering i förhållande till den nya lagen. Fram till 2001 då personuppgiftslagen trädde i full kraft antogs ett flertal nya s.k. registerförfattningar. Vissa av dem har en annorlunda utformning än tidigare reglering på så sätt att de inte är begränsade till att avse viss behandling av personuppgifter i traditionella register, utan i stället gäller generellt på helt eller delvis automatiserad personuppgiftsbehandling inom en viss verksamhet.

Trots att begreppet *registerförfattning* avser mer än reglering av utpräglade personregister brukar det användas som ett samlingsnamn för författningar som innehåller någon form av särreglering av personuppgiftsbehandling i förhållande till personuppgiftslagen. Informationshanteringsutredningen har i sitt betänkande *Myndighetsdatalag* (SOU 2015:39) gjort en kartläggning av registerförfattningar. I betänkandet beskrivs att registerförfattningar kan delas in i tre kategorier: renodlade registerförfattningar, informationshanteringsförfattningar och andra författningar med inslag av dataskyddsbestämmelser.⁶ Bland de författningar som ingår i vårt uppdrag förekommer författningar i alla tre kategorierna.

⁵ Prop. 1997/98:44 s. 41 och vidare prop. 1990/91:60 s. 50 och KU 1990/91:11 s. 11.

⁶ SOU 2015:39 s. 96–105.

När det gäller frågan om och hur förhållandet till personuppgiftslagen ska regleras i en registerförfattning har det valts olika lösningar i skilda registerförfattningar. Ett sätt är att personuppgiftslagen inte nämns alls i registerförfattningen. Detta innebär då att registerförfattningens reglering gäller framför personuppgiftslagen, i den mån författningen kan uppfattas som avvikande från den lagen. Samma förhållande kommer att gälla om det i registerförfattningen uttryckligen anges att lagen gäller *utöver* personuppgiftslagen. En sådan bestämmelse har alltså i första hand ett informativt syfte. I andra registerförfattningar, särskilt för myndigheter med brottsbekämpande uppdrag, har det i stället angetts att den aktuella registerlagen gäller *i stället för* personuppgiftslagen, utom avseende de bestämmelser i personuppgiftslagen som särskilt räknas upp. Fördelen med den lösningen har ansetts vara att lagstiftningen blir överskådlig, tydlig och mer lättillämpad.⁷

2.3 EU:s dataskyddsreform

2.3.1 Tidigare EU-rättsakter

I artikel 8 i EU:s stadga om de grundläggande rättigheterna (rättighetsstadgan) finns rätten till skydd av personuppgifter. Sådana uppgifter ska behandlas lagenligt för bestämda ändamål och på grundval av samtycke eller någon annan lagenlig grund. Inskränkningar i stadgans rättigheter får göras i lag och ska vara förenliga med det väsentliga innehållet i rättigheterna, de får bara göras om de är nödvändiga och svarar mot ett allmänt samhällsintresse som erkänns av unionen eller behovet av skydd för andra människors rättigheter och friheter.

Den allmänna regleringen av behandling av personuppgifter inom EU finns i dag i 1995 års dataskyddsdirektiv. Direktivet har, som nämnts, genomförts i svensk rätt genom personuppgiftslagen.

Dataskyddsdirektivet gäller inte inom medlemsstaternas verksamhet på straffrättens område (artikel 3). Inom detta område finns dock flera andra EU-rättsakter som reglerar informations-

⁷ Se exempelvis prop. 2009/10:85 s. 80.

utbyte mellan medlemsstaterna och som innehåller bestämmelser om dataskydd, bl.a. rådets rambeslut 2008/977/RIF av den 27 november 2008 om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete (dataskyddsrambeslutet).⁸ Genom dataskyddsrambeslutet infördes en generell reglering av dataskydd på det polisiära och straffrättsliga området. Dataskyddsrambeslutet gäller dock endast för personuppgifter som överförs mellan medlemsstaterna och inte för behandlingen av personuppgifter på nationell nivå. Dataskyddsrambeslutet har genomförts i svensk rätt främst genom lagen (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen med tillhörande förordning.⁹

2.3.2 Reformen – två nya EU-rättsakter om personuppgiftsbehandling

Inom EU har länge pågått ett arbete med att ta fram ett nytt regelverk för personuppgiftsbehandling för att ersätta 1995 års dataskyddsdirektiv och dataskyddsrambeslutet. Resultatet har blivit två nya rättsakter – Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (kallas *dataskyddsförordningen* i det följande) och 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 (kallas *det nya dataskyddsdirektivet* i det följande).

Dataskyddsförordningen ska börja tillämpas den 25 maj 2018. Den är en ny generell reglering för behandling av personuppgifter inom EU och upphäver 1995 års dataskyddsdirektiv. I egenskap av förordning har den allmän giltighet och är bindande och direkt

⁸ För fler exempel, se SOU 2017:29 s. 155–157.

⁹ Prop. 2012/13:73.

tillämplig i medlemsstaterna. En första följd av att förordningen ska börja tillämpas är att personuppgiftslagen måste upphävas. Vidare får inte andra författningar inom förordningens tillämpningsområde innehålla bestämmelser som motsvarar förordningens reglering, eftersom en förordning, till skillnad från ett direktiv, inte ska genomföras i nationell rätt. Även om dataskyddsförordningen är direkt tillämplig, innehåller den många bestämmelser som förutsätter eller ger utrymme för kompletterande nationella bestämmelser av olika slag. I skälen till förordningen anges också att om förordningen föreskriver förtydliganden eller begränsningar av dess bestämmelser genom medlemsstaternas nationella rätt, kan medlemsstaterna, i den utsträckning det är nödvändigt för samstämmigheten och för att göra de nationella bestämmelserna begripliga för de personer som de tillämpas på, införliva delar av förordningen i nationell rätt.¹⁰

Förordningen baseras till stor del på den struktur och reglering som finns i 1995 års dataskyddsdirektiv. Förordningen anses dock innebära ett starkare skydd för den enskilde, bl.a. genom att regleringen av den enskildes rättigheter och den personuppgiftsansvariges skyldigheter utvecklats.

Från förordningens tillämpningsområde undantas personuppgiftsbehandling som utförs av behöriga myndigheter i syfte att förebygga, utreda, upptäcka eller lagföra brott eller verkställa straffrättsliga påföljder samt att skydda och förebygga hot mot den allmänna säkerheten. Sådan personuppgiftsbehandling omfattas i stället av det nya dataskyddsdirektivets tillämpningsområde.

Det nya dataskyddsdirektivet ska vara genomfört i nationell rätt senast den 6 maj 2018. Det ansluter i stora delar till det tidigare dataskyddsrambeslutet, men är tillämpligt både på enbart nationell personuppgiftsbehandling och på personuppgiftsbehandling som avser ett informationsutbyte mellan medlemsstater.¹¹ Genom direktivet upphävs dataskyddsrambeslutet. Eftersom även dataskyddsrambeslutet till stora delar är baserat på 1995 års dataskyddsdirektiv innehåller det nya dataskyddsdirektivet en reglering

¹⁰ Jfr SOU 2017:39 s. 72 f. Dataskyddsutredningen anmärker att förordningen har en "direktivliknande" karaktär.

¹¹ SOU 2017:29 s. 121.

som på många områden överensstämmer med dataskyddsförordningens.¹²

Viss behandling av personuppgifter undantas från både det nya dataskyddsdirektivets och dataskyddsförordningens tillämpningsområde. Det gäller bl.a. personuppgiftsbehandling i verksamhet som inte omfattas av unionsrätten (artikel 2 i respektive rättsakt).

2.3.3 Förslaget till dataskyddslag

Dataskyddsförordningen är alltså direkt tillämplig i medlemsstaterna. Samtidigt både förutsätter och möjliggör den kompletterande nationella bestämmelser av olika slag. En särskild utredare har haft uppdraget att föreslå de anpassningar och kompletterande författningsbestämmelser på generell nivå som dataskyddsförordningen ger anledning till (dir. 2016:15). Utredningen har antagit namnet Dataskyddsutredningen och har den 12 maj 2017 överlämnat betänkandet *Ny dataskyddslag* (SOU 2017:39).

Den föreslagna dataskyddslagen innehåller bestämmelser om rättslig grund (2 kap), vissa kategorier av personuppgifter (3 kap.), användningsbegränsningar (4 kap.), begränsningar av vissa rättigheter och skyldigheter (5 kap.), tillsynsmyndighetens handläggning och beslut (6 kap.), administrativa sanktionsavgifter (7 kap.) och skadestånd och rättsmedel (8 kap.). Vissa bestämmelser i lagen överensstämmer i huvudsak med personuppgiftslagens eller personuppgiftsförordningens reglering.

Dataskyddslagen föreslås vara subsidiär till annan författning (1 kap. 3 §). I den mån dataskyddsförordningen medger det kan alltså andra författningar innehålla avvikande bestämmelser i förhållande till dataskyddslagen.

Genom den föreslagna lagen upphävs personuppgiftslagen. Dataskyddslagen föreslås träda i kraft den 25 maj 2018.

¹² Om 1995 års dataskyddsdirektivs inverkan på dataskyddsrambeslutet, se prop. 2012/13:73 s. 56.

2.3.4 Förslaget till brottsdatalag m.m.

En särskild utredare har haft i uppdrag att föreslå hur det nya dataskyddsdirektivet ska genomföras i svensk rätt (dir.2016:21). Utredningen om 2016 års dataskyddsdirektiv har lämnat förslag till en ny ramlag med bestämmelser om skydd av personuppgifter inom direktivets tillämpningsområde i sitt delbetänkande *Brottsdatalag* (SOU 2017:29). Brottsdatalagen innehåller bestämmelser om bl.a. den personuppgiftsansvariges skyldigheter (3 kap.), enskildas rättigheter (4 kap.), tillsyn (5 kap.), administrativa sanktionsavgifter (6 kap.), skadestånd och rättsmedel (7 kap.) och överföring av personuppgifter till tredjeland och internationella organisationer (8 kap.). I sitt slutbetänkande *Brottsdatalag – kompletterande bestämmelser* (SOU 2017:74) lämnar utredningen förslag till anpassningar av flera registerförfattningar inom det nya dataskyddsdirektivets tillämpningsområde, bl.a. polisdatalagen (2010:361).

2.3.5 Något om gränsdragningen mellan direktivet och förordningen

Utredningen om 2016 års dataskyddsdirektiv redovisar i kapitel 8 i sitt betänkande *Brottsdatalag* (SOU 2017:29) några ställningstaganden när det gäller brottsdatalagens, och därmed det nya dataskyddsdirektivets, närmare tillämpningsområde. Redovisningen är dock inte avsedd att vara uttömmande.¹³

För att brottsdatalagen ska vara tillämplig, och inte dataskyddsförordningen, ska behandlingen utföras både av en behörig myndighet och med ett sådant syfte som närmare framgår av brottsdatalagen. Detta innebär bl.a. att avgränsningen inte går att göra med utgångspunkt enbart i att en viss personuppgiftsbehandling utförs av en myndighet vars huvudsakliga uppgift är t.ex. brottsbekämpning. Inte heller typen av personuppgiftsbehandling eller personuppgiftens karaktär i och för sig är avgörande. Utredningen om 2016 års direktiv konstaterar bl.a. att kontrollverksamhet inte faller under brottsdatalagens tillämp-

¹³ SOU 2017:29 s. 181.

ningsområde och inte heller allmän övervakning, även om den utförs av myndigheter som också har brottsbekämpande uppdrag.¹⁴

Precis som registerförfattningar i dag kompletterar personuppgiftslagen kommer registerförfattningar att i framtiden komplettera antingen dataskyddsförordningen eller brottsdatalagen, som är den lag som på en generell nivå kommer att genomföra dataskyddsdirektivet. Det är också möjligt att en registerförfattning kompletterar både dataskyddsförordningen och brottsdatalagen. Inom ramen för samma registerförfattning kan man nämligen tänka sig att det förekommer personuppgiftsbehandling som faller under antingen den ena eller den andra EU-rättsakten.¹⁵ Samma behandling kan dock inte falla under båda EU-rättsakterna samtidigt.¹⁶

EU-rättsakterna har flera likheter. Bl.a. är det möjligt att behålla många bestämmelser i myndigheternas registerförfattningar oavsett vilken EU-rättsakt som är tillämplig. Rättsföljderna för den enskilde behöver inte heller skilja sig åt när det gäller exempelvis möjligheten att begära rättelse eller skadestånd. Skyldigheterna för personuppgiftsansvariga kommer troligtvis att kunna uppfyllas genom i huvudsak samma åtgärder. Trots detta är det naturligtvis väsentligt för myndigheterna att veta om det är dataskyddsförordningen eller brottsdatalagen som är det generellt tillämpliga regelverket.

Vi har anledning att återkomma till frågor om gränsdragning i flera avsnitt i denna promemoria.

2.4 Vårt uppdrag och dess genomförande

Uppdragsbeskrivningen

I vår uppdragsbeskrivning anges att vi ska undersöka vilka anpassningar som är behövliga eller lämpliga och lämna förslag på de författningsändringar som EU:s dataskyddsreform föranleder i fråga om den personuppgiftsreglering som Enheten för lagstiftning om allmän ordning och säkerhet och samhällets krisberedskap vid

¹⁴ A. a. s. 184.

¹⁵ Jfr Fi2017/02899/S3 s. 48, 124 f och 135.

¹⁶ SOU 2017:29. s. 172 och 182, jfr även s. 292.

Justitiedepartementet (Enheten) ansvarar för. Under uppdragets gång har Enheten preciserat vilka författningar som ingår i vårt uppdrag. Några andra mer detaljerade anvisningar följer inte av vår uppdragsbeskrivning, utan där sägs endast att uppdraget omfattar att analysera både dataskyddsförordningen och det nya dataskyddsdirektivet i förhållande till de författningar som Enheten ansvarar för men som inte omfattas av de uppdrag som Dataskyddsutredningen eller Utredningen om 2016 års dataskyddsdirektiv har.

Vi har, i enlighet med vårt uppdrag, särskilt samrått med Utredningen om 2016 års dataskyddsdirektiv, Polismyndigheten och Kustbevakningen.

Avgränsning av vårt uppdrag

Vi har uppfattat att en grundläggande utgångspunkt för vårt uppdrag är att den författningsreglering som för närvarande finns avseende personuppgiftsbehandling ska behållas oförändrad i så stor utsträckning som det är möjligt, dvs. om inte dataskyddsförordningen eller det nya dataskyddsdirektivet kräver att nationella bestämmelser måste upphävas eller ändras. Förordningen är direkt tillämplig och nationella bestämmelser som reglerar samma sak som förordningen kan därmed inte kvarstå, utan förordningen ska tillämpas i stället. Direktivet ska däremot genomföras i svensk rätt och svensk rätt kan därmed reglera samma områden som direktivet, men regleringen ska i sådana fall genomföra direktivet och får inte strida emot vad som föreskrivs där.

Vi anser som en utgångspunkt att det inte ingår i vårt uppdrag att ompröva sådana redan gjorda ställningstaganden och överväganden som fortfarande är relevanta. Det gäller bl.a. överväganden om behovet av en särreglering och vad denna i huvudsak bör innehålla.

Förhållandet till andra utredningar

Det finns ett stort antal registerförfattningar i svensk rätt. Bara inom Justitiedepartementet har det funnits behov att tillsätta flera utredningar att närmare analysera inverkan av EU:s dataskydds-

reform på olika författningar inom enhetens ansvarsområde. Vi har tagit del av andra utredningars arbete och har deltagit i samrådsmöten där utredningar från alla departement har haft möjlighet att delta. Vi har också diskuterat under hand med andra utredningar. Eftersom antalet andra utredningar varit så stort har det varit omöjligt att närmare ta till sig eller försöka anpassa sig till alla förslag och överväganden som redan offentligt redovisats eller framkommit under hand. Vi har i första hand tagit del av och beaktat Dataskyddsutredningen och Utredningen om 2016 års dataskyddsdirektiv.

När det gäller förslaget till brottsdatalog (av Utredningen om 2016 års dataskyddsdirektiv, SOU 2017:29) och förslaget till dataskyddslag (av Dataskyddsutredningen, SOU 2017:39) refererar vi till dem utan att varje gång särskilt ange att det handlar om författningsförslag och inte antagna lagar, detta för att inte tynga framställningen i onödan. Det är dock givet att ändringar och justeringar kan komma att göras i respektive lagförslag, och våra överväganden och förslag får då bedömas därefter.

2.5 Allmänna överväganden om anpassningen av registerförfattningar till dataskyddsförordningen

2.5.1 Dataskyddsförordningens tillämpningsområde

Dataskyddsförordningens tillämpningsområde framgår av artikel 2. Förordningen omfattar för det första behandling av personuppgifter som helt eller delvis företas på automatisk väg samt på annan behandling än automatisk av personuppgifter som ingår i eller kommer att ingå i ett register. Vad som avses med ett register framgår av definitionerna i artikel 4.6. Denna avgränsning av förordningens tillämpningsområde förorsakar inte några tolkningsproblem såvitt avser de författningar som ingår i vårt uppdrag – det framgår av författningarna att de reglerar sådan personuppgiftsbehandling som är helt eller delvis automatiserad och/eller avser regelrätta register. Samtliga författningar som ingår i vårt uppdrag avser personuppgiftsbehandlingen vid olika myndigheter. Det undantag från dataskyddsförordningens tillämpningsområde som anges i artikel 2.2 c – behandling som en fysisk person utför i

verksamhet av rent privat natur – är alltså inte aktuellt inom ramen för vår översyn.

En annan fråga är den närmare innebörden av dataskyddsförordningens tillämpningsområde som följer av artikel 2.2 a. Dataskyddsförordningen är enligt denna del av artikeln inte tillämplig på personuppgiftsbehandling som utförs i en verksamhet som inte omfattas av unionsrätten.

Dataskyddsutredningen anför att det i viss mån är oklart hur tillämpningsområdet i denna del ska tolkas. Utredningen menar att det inom offentlig sektor kan finnas områden som inte omfattas av unionsrätten på ett sådant sätt som gör undantaget från tillämpningsområdet tillämpligt.¹⁷ Dataskyddsutredningen föreslår dock att dataskyddsförordningen i svensk rätt ska gälla även inom områden som undantas enligt artikel 2.2 a (och b) (1 kap. 2 § dataskyddslagen). Ett skäl till detta är att även personuppgiftslagen haft ett sådant vidare tillämpningsområde i förhållande till 1995 års dataskyddsdirektiv. Ett annat skäl är att Sverige har gjort vissa andra internationella åtaganden att skydda enskilda individers personliga integritet som gör att det finns ett behov av en generellt tillämplig dataskyddsreglering.¹⁸

Vår utgångspunkt vid översynen av författningarna har varit att de registerförfattningar vi ska analysera omfattas av dataskyddsförordningens tillämpningsområde, utom i de fall de i stället omfattas av det nya dataskyddsdirektivet.

2.5.2 Rättslig grund för personuppgiftsbehandlingen

Den europeiska dataskyddsregleringen utgår från att varje behandling av personuppgifter måste ha en rättslig grund. I dataskyddsförordningen räknas dessa rättsliga grunder upp i artikel 6.1. Behandling är enligt artikeln endast laglig om åtminstone ett av de uppräknade villkoren (punkterna a–f) är uppfyllt. De olika villkoren är i viss mån överlappande. Flera av punkterna a–f kan därför vara tillämpliga samtidigt avseende en och samma behandling.¹⁹

¹⁷ SOU 2017:39 s. 91, jfr Fi2017/02899/S3 s. 47 f. och Ds 2017:19 s. 102 f.

¹⁸ SOU 2017:39. s. 92.

¹⁹ A. a. s. 103 f.

De statliga och kommunala myndigheternas personuppgiftsbehandling kommer huvudsakligen att ske med stöd av de rättsliga grunder som kommer till uttryck i artikel 6.1 c eller e (eller båda) i dataskyddsförordningen. Enligt artikel 6.1 c är personuppgiftsbehandling laglig om den är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige. Enligt artikel 6.1 e gäller att behandlingen är laglig om den är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.

Gemensamt för artikel 6.1 c och e är att personuppgiftsbehandling ska vara *nödvändig* för att vara laglig. Dataskyddsutredningen har närmare utvecklat vad som kan anses ligga i detta begrepp. Sammanfattningsvis anför utredningen att det inte kan innebära att det krävs att det är omöjligt att utföra exempelvis uppgiften av allmänt intresse utan att behandla personuppgifter, utan att det räcker med att personuppgiftsbehandlingen medför effektivitetsvinster.²⁰

När det gäller vad som avses med en uppgift av *allmänt intresse* anför Dataskyddsutredningen att det, med hänsyn till svensk förvaltningstradition, förefaller rimligt att anta att alla uppgifter som utförs av statliga myndigheter i syfte att uppfylla ett uttryckligt uppdrag av riksdag eller regeringen är av allmänt intresse.²¹

Myndigheternas verksamhet omfattar ofta myndighetsutövning. Eftersom det i de flesta fall är tillräckligt att konstatera att myndigheten utför ett uppdrag av allmänt intresse som kräver personuppgiftsbehandling, anser vi inte att det är nödvändigt att i vår utredning närmare analysera i vilken omfattning olika myndigheters verksamhet innefattar myndighetsutövning. Dataskyddsutredningen har närmare utvecklat hur begreppet bör tolkas.²²

När det slutligen gäller utförandet av en *rättslig förpliktelse* anför Dataskyddsutredningen att ett exempel på en sådan förpliktelse för en myndighet är de skyldigheter som följer av offentlighetsprincipen. Myndigheters uppdrag kan också innebära rättsliga förpliktelser, exempelvis då myndigheten ges i uppdrag att föra ett visst register.²³

²⁰ SOU 2017:39. 105 f.

²¹ A. a. s. 124.

²² A. a. s. 119 f.

²³ A. a. s. 117.

De rättsliga grunder som räknas upp i artikel 6.1 är i huvudsak desamma som sedan tidigare gällt enligt artikel 7 i 1995 års dataskyddsdirektiv, som genomförts i 10 § personuppgiftslagen. Man bör därför som en utgångspunkt kunna förlita sig på att lagstiftaren redan tagit ställning till att personuppgiftsbehandling som regleras i en viss registerförfattning är nödvändig för att en myndighet ska kunna utföra ett uppdrag av allmänt intresse, som ett led i myndighetsutövning eller för att fullgöra en rättslig förpliktelse.

En nyhet i förhållande till dataskyddsdirektivet när det gäller rättsliga grunder är det tillkommande kravet i artikel 6.3 på att de rättsliga grunderna enligt artikel 6.1 c och e ska *fastställas i unionsrätten eller i nationell rätt*. Dataskyddsutredningen har haft i uppdrag att analysera vad kravet i denna del innebär i fråga om nationell författningsreglering.²⁴ Dataskyddsutredningen anför sammanfattningsvis att detta krav inte kan uppfattas så att det måste finnas en författningsreglering av själva personuppgiftsbehandlingen. Det är i stället uppgiften av allmänt intresse, myndighetsutövningen eller den rättsliga förpliktelsen som måste ha stöd i nationell rätt (eller unionsrätten). Att den rättsliga grunden ska ha stöd i nationell rätt innebär inte nödvändigtvis att den måste vara fastställd i en av riksdagen beslutad lag. Däremot måste den vara fastställd i laga ordning, på ett konstitutionellt korrekt sätt.²⁵

Dataskyddsutredningen anför följande angående den rättsliga grunden i 6.1 e (uppdrag av allmänt intresse) och frågan om kravet på att den ska ha stöd i nationell rätt.

Myndigheternas uppdrag och åligganden framgår av författningar, regeringsbeslut och kommunala reglementen, antagna i enlighet med grundlagens bestämmelser om normgivningskompetens och kommunalt självstyre. De åtgärder som myndigheterna vidtar i syfte att utföra dessa uppdrag eller uppfylla dessa åligganden har därmed i sig en legal grund, som har offentliggjorts genom tydliga, precisa och förutsebara regler. Nödvändig behandling av personuppgifter kan därmed ske med stöd av artikel 6.1 e i dataskyddsförordningen.²⁶

I artikel 6.3 andra stycket anges också att syftet med behandlingen måste vara nödvändigt för att utföra en uppgift av allmänt intresse. Dataskyddsutredningen anför att detta innebär att den specifika

²⁴ SOU 2017:39 s. 103.

²⁵ A. a. s. 112.

²⁶ A. a. s. 128 f.

behandlingen alltså måste vara nödvändig för ett ändamål som i sin tur är nödvändigt för att myndigheten ska kunna utföra sitt uppdrag.²⁷

När det gäller rättsliga förpliktelser ska dessa också, på samma sätt som uppdrag av allmänt intresse, vara fastställda i nationell rätt (eller unionsrätt). När det gäller sådana förpliktelser ställer artikel 6.3 upp ytterligare ett krav, nämligen att *syftet med behandlingen* ska fastställas i den rättsliga grunden. Dataskyddsutredningen anför att syftet med behandlingen alltså ska vara bestämt av den författning som anger eller ger stöd för förpliknelsen. Detta, menar utredningen, innebär att förpliknelsen inte får vara alltför svepande eller ge den personuppgiftsansvarige en alltför stor handlingsfrihet i fråga om hur förpliknelsen ska uppfyllas.²⁸

Slutligen ställer artikel 6.3 särskilda krav på den nationella rätt (eller EU-rätt) som fastställer den rättsliga grunden, nämligen att den ska uppfylla ett mål av allmänt intresse och vara proportionell mot de legitima mål som eftersträvas. Vi återkommer till detta krav nedan.

I vårt uppdrag ingår att analysera ett antal författningar som reglerar personuppgiftsbehandling som utförs av myndigheter. När personuppgiftsbehandling särskilt regleras för en myndighet utgår regleringen ofta från myndighetens, redan författningsreglerade, uppdrag. Redan av vad som redogjorts för ovan kan man övergripande konstatera att sådan personuppgiftsbehandling inte bara uppfyller kraven i artikel 6.1 c eller e (eller båda) utan också är ”fastställd” i nationell rätt, både genom författningsregleringen av myndighetsuppdraget och genom den författning som närmare reglerar personuppgiftsbehandlingen. Ändamålet med behandlingen har därmed också redan av riksdag eller regering satts i den nödvändiga relationen till utförandet av uppdraget av allmänt intresse och/eller till myndighetsutövningen. Eftersom kravet på att den rättsliga grunden ska vara fastställd i nationell rätt (eller unionsrätt) är nytt i förhållande till 1995 års dataskyddsdirektiv, gör vi dock inledningsvis för varje författning en kortfattad bedömning av om de rättsliga förutsättningarna för personuppgiftsbehandling i enlighet med artikel 6.1 c eller e och 6.3 är

²⁷ SOU 2017:39 s. 129.

²⁸ A. a. s. 114.

uppfyllda. Vi gör dock ingen bedömning av om författningsregleringen i sig är till för att uppfylla ett mål av allmänt intresse eller om den är proportionell i förhållande till detta mål. Att göra den typen av överväganden anser vi i princip inte ingår i vårt uppdrag (jfr avsnitt 2.4) och man måste dessutom kunna utgå ifrån att redan antagna författningar uppfyller dessa krav.²⁹

2.5.3 Övergripande om möjligheten att behålla och införa särreglering

Enligt artikel 6.2 får medlemsstaterna behålla eller införa mer specifika bestämmelser för att anpassa tillämpningen av bestämmelserna i förordningen för behandling som sker med stöd av artikel 6.1 c och e genom att ”närmare fastställa specifika krav för uppgiftsbehandlingen och andra åtgärder för att säkerställa en laglig och rättvis behandling”. Möjligheten för medlemsstaterna att föreskriva mer specifika regler för behandlingen av personuppgifter framgår också av artikel 6.3. Artikeln anger att den nationella rättsliga grunden för behandling enligt artikel 6.1 c och e kan innehålla bland annat de allmänna villkor som ska gälla för den personuppgiftsansvariges behandling, vilken typ av uppgifter som ska behandlas, vilka registrerade som berörs samt de enheter till vilka personuppgifterna får lämnas ut och för vilka ändamål. I den rättsliga grunden får också anges ändamålsbegränsningar, lagringstid samt typer av behandling och förfaranden för behandling inbegripet åtgärder för att tillförsäkra en laglig och rättvis behandling, däribland för behandling i andra särskilda situationer enligt kapitel IX. Det nämnda kapitlet innehåller bl.a. bestämmelser om behandling av nationella identifikationsnummer.

Bestämmelser i registerförfattningar avser ofta just sådana områden som nämns i denna del av artikel 6.3. Av både artikel 6.2 och 6.3 följer alltså att det är tillåtet att nationellt reglera olika aspekter av personuppgiftsbehandling inom offentlig sektor i registerförfattningar.³⁰ Förordningen innehåller också andra artiklar som tillåter kompletterande bestämmelser i vissa avseenden, exempelvis när det gäller särskilda kategorier av person-

²⁹ Jfr SOU 2017:66 s. 206.

³⁰ Jfr SOU 2017:39 s. 134.

uppgifter (artikel 9.2 g) och inskränkningar av den registrerades rättigheter (artikel 23).

Dataskyddsförordningen sätter upp de ramar inom vilka personuppgiftsbehandling är tillåten. Den innebär dock givetvis ingen skyldighet att behandla personuppgifter, även om alla förutsättningar att utföra personuppgiftsbehandling är uppfyllda i och för sig. Det står därmed lagstiftaren fritt att begränsa offentlig sektors behandling av personuppgifter i förhållande till dataskyddsförordningen. Ett exempel är att det inte finns något hinder emot att i författning ange att en myndighet inte får behandla personuppgifter annat än för vissa uttömmande angivna ändamål och alltså förhindra att myndigheten självständigt tillämpar den s.k. finalitetsprincipen (som innebär att personuppgifter insamlade för ett visst ändamål endast får behandlas för ett annat ändamål under förutsättning att de nya ändamålen inte är oförenliga med det ändamål för vilket uppgifterna samlades in – principen framgår bl.a. av artikel 5.1 b dataskyddsförordningen). Eftersom det är riksdag och regering som fastställer omfattningen av myndigheternas uppdrag finns det heller inget hinder emot att en myndighet ges mer långtgående skyldigheter när det gäller skyddet för den registrerade i något avseende. Exempelvis skulle en författning kunna ge myndigheten i uppdrag att ge den registrerade mer information än vad som följer av dataskyddsförordningen.³¹

2.5.4 Bestämmelser som är förenliga med dataskyddsförordningen

Syfte och tillämpningsområde

En del registerförfattningar inleds med en allmän bestämmelse som anger syftet med lagstiftningen. Syftet kan vara exempelvis både att möjliggöra personuppgiftsbehandling och samtidigt skydda människors personliga integritet. Sådana bestämmelser har inget direkt

³¹ Jfr Fi2017/02899/S3 s. 57 f., SOU 2017:66 s. 203 och Ds 2017:41 s. 62 f. En annan sak är att det skulle strida mot dataskyddsförordningen om det allmänna på något sätt, exempel i författning, skulle inskränka de principer enligt vilka en privat aktör enligt dataskyddsförordningen har rätt att behandla personuppgifter, jfr EU-domstolens dom i mål C-582/14 och i de förenade målen C-468/10 och C-469/10.

materiellt innehåll och utgör i sig ingen reglering av den förekommande personuppgiftsbehandlingen. De kan därför behållas.

Även bestämmelser som avgränsar tillämpningsområdet för en viss registerförfattning kan behållas. Eftersom särreglering är möjlig enligt förordningen måste givetvis den nationella lagstiftaren kunna specificera inom vilket område eller för vilken personuppgiftsbehandling en viss särreglering gäller.³²

I avgränsningen av tillämpningsområdet anges vanligen också att lagen endast tillämpas på helt eller delvis automatiserad personuppgiftsbehandling, eller annan behandling om personuppgifterna ingår eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier. Dataskyddsförordningen har samma tillämpningsområde när det gäller formerna för behandling. Eftersom det också är möjligt att i nationell rätt specificera frågor om personuppgiftsbehandling för en mer avgränsad form av behandling (exempelvis endast för behandling i ett visst automatiserat register) menar vi att det sedvanliga sättet att ange vilka former av behandling som omfattas av tillämpningsområdet för en viss registerförfattning är förenligt med dataskyddsförordningen, i vart fall med beaktande av skäl 8. En annan fråga är om denna avgränsning av tillämpningsområdet numera är överflödig, särskilt om en hänvisning till dataskyddsförordningen införs i författningen. Vi menar dock att det fortfarande fyller en funktion att avgränsa tillämpningsområdet på detta sätt med tanke på att en begränsning av det också varit möjlig. Det blir också tydligare att ingen materiell ändring i tillämpningsområdet är avsedd.³³

I vissa registerförfattningar kan bestämmelserna för personuppgiftsbehandling vara tillämpliga även på andra typer av uppgifter, exempelvis avseende juridiska personer. Sådana bestämmelser påverkas inte av dataskyddsförordningen, eftersom den inte innehåller reglering avseende något annat än personuppgifter.³⁴

³² Jfr SOU 2017:66 s. 207–209.

³³ Utredningen om 2016 års dataskyddsdirektiv har till exempel inte med motsvarande avgränsning i de registerförfattningar som omfattas av deras uppdrag. Avgränsningen framgår i stället av brottsdatalagen, som registerförfattningarna gäller utöver. Jfr vidare Fi2017/02899/S3 s. 65 f. och SOU 2017:66 s. 209.

³⁴ Jfr Fi2017/02899/S3 s. 65 f. och SOU 2017:66 s. 209.

Personuppgiftsansvar

Registerförfattningar anger ofta vem som är personuppgiftsansvarig.

Av definitionen i artikel 4.7 i dataskyddsförordningen framgår att personuppgiftsansvarig är en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter. Om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt. Det står alltså klart att bestämmelser som preciserar personuppgiftsansvaret inte förhindras av förordningen.³⁵

Ändamålsbestämmelser

Att föreskriva för vilka ändamål personuppgiftsbehandling får utföras kan allmänt ses som en precisering av vilken personuppgiftsbehandling som är tillåten. Ändamålsbestämmelser skulle kunna inordnas under medlemsstaternas allmänna möjlighet enligt artikel 6.2 att införa eller behålla ”mer specifika bestämmelser för att anpassa tillämpningen av bestämmelserna” i förordningen när det gäller behandling som grundar sig på artikel 6.1 c och e. En av principerna för personuppgiftsbehandling enligt förordningen är att behandling bara ska ske för särskilda, uttryckligt angivna och berättigade ändamål (artikel 5.1 b). Ändamålsbegränsningar nämns också i artikel 6.3 som exempel på reglering som den rättsliga grunden för personuppgiftsbehandling kan innehålla. Dataskyddsutredningen konstaterar att förordningen inte kan anses ställa krav på att ändamål anges i nationell författning, men att den heller inte förhindrar en sådan ordning.³⁶

I många fall torde ändamålsreglering kunna ses som inte bara en precisering av vad som gäller för personuppgiftsbehandlingen, utan också som (en del av) den rättsliga grunden för behandling i

³⁵ Jfr exempelvis SOU 2017:66 s. 213 f., Ds 2017:28 s. 108 f. och Ds 2017:19 s. 125 f.

³⁶ SOU 2017:39 s. 107.

enlighet med artikel 6.1 c och e. Inom ramen för sitt uppdrag att genomföra det nya dataskyddsdirektivet har Utredningen om 2016 års dataskyddsdirektiv väckt frågan om inte ändamålsbestämmelser snarast ska ses som rättsliga grunder för behandlingen och inte som en reglering av den ändamålsbestämning som ska göras för varje enskild behandling. Samma synsätt skulle i och för sig vara möjligt även beträffande ändamålsreglering inom dataskyddsförordningens tillämpningsområde. Vi återkommer till denna fråga i avsnitt 3.5.3 Oavsett hur man ser på ändamålsbestämmelser i detta avseende menar vi att det står klart att de, även i sin nuvarande utformning, är förenliga med dataskyddsförordningen.³⁷

I vissa författningar kategoriseras ändamålen som primära och sekundära ändamål. Primära ändamål är utformade för att tillgodose myndighetens behov av att samla in och vidarebehandla personuppgifter i den verksamhet som omfattas av den aktuella registerförfattningens tillämpningsområde. Sekundära ändamål beskriver för vilka ändamål uppgifter får vidarebehandlas för att kunna lämnas ut, i första hand till andra myndigheter. De avser alltså att tillgodose behovet av information i en annan verksamhet än den egna. (Med vidarebehandling avses i det följande behandling för ett annat ändamål än det för vilket uppgifterna samlades in.)

Att primära och sekundära ändamålsbestämmelser reglerar vidarebehandling kan ses som en precisering av finalitetsprincipen och därmed även på den grunden anses förenliga med artikel 6.2.³⁸ Just när det gäller vidarebehandling anser vi att det även bör uppmärksammas att artikel 6.4 tycks ställa särskilda krav på nationell rätt. Av bestämmelsen framgår att om nationell rätt medger vidarebehandling behöver inte den personuppgiftsansvarige göra någon självständig bedömning av om ett nytt ändamål är förenligt med det ursprungliga behandlingsändamålet. I artikeln anges dock att det i så fall ska vara fråga om nationell rätt som är en nödvändig och proportionell åtgärd i ett demokratiskt samhälle för att skydda de mål som avses i artikel 23.1. Målen räknas upp i artikeln i punkterna a–j. Vissa är tämligen specifikt angivna, såsom nationell säkerhet eller tillsyn över myndighetsutövning. Det mest

³⁷ Jfr även exempelvis Ds 2017:33 s. 95 f., Ds 2017:28 s. 103 och SOU 2017:66 s. 224.

³⁸ Se exempelvis prop. 2011/12:45 s. 103. Även sekundära ändamålsbestämmelser som kan anses tillåta vidarebehandling för *oförenliga* ändamål torde kunna ses som förenliga med dataskyddsförordningen med stöd av skäl 50, se vidare Fi2017/02899/S3 s. 55 f.

generella målet, punkten e, torde vara det som oftast kommer i fråga för vidarebehandling av en myndighet. Det avser ett av "unionens eller en medlemsstats viktiga mål av generellt allmänt intresse". Eftersom både den utlämnande och den mottagande myndigheten i allmänhet får anses grunda sin personuppgiftsbehandling på artikel 6.1 e (ett uppdrag av allmänt intresse) är frågan om det nu nämnda kravet på ett *viktigt mål av allmänt intresse* tillför något utöver vad som redan följer av att personuppgiftsbehandlingen i allmänhet ska vara laglig. Möjligen kan uttrycket *viktigt* i sammanhanget uppfattas så. Dataskyddsutredningen har med anledning av ett annat krav på viktigt allmänt intresse, det i artikel 9.2 g, anfört att ett viktigt allmänintresse är att svenska myndigheter kan bedriva den verksamhet som tydligt faller inom ramen för deras uppdrag på ett korrekt, rättssäkert och effektivt sätt. Även om uttryckssätten är något olika i artikel 23.1 e och artikel 9.2 g, anser vi att man med ledning av utredningens uttalande kan dra slutsatsen att sekundära ändamålsbestämmelser som avser myndigheters möjlighet att vidarebehandla personuppgifter får anses ha syften som motsvarar det som avses med viktiga mål av generellt allmänt intresse i artikel 23.1 e. Sekundära ändamålsbestämmelser får alltså i allmänhet anses förenliga även med dataskyddsförordningens artikel 6.4.³⁹

Slutligen kan särskilt anmärkas att en sekundär ändamålsbestämmelse inte sällan har innebörden att uppgifter får behandlas för att lämnas vidare till en i det nya dataskyddsdirektivets mening behörig myndighet i syfte att bekämpa brott, eller något annat sådant syfte som omfattas av det nya dataskyddsdirektivets tillämpningsområde. Att en sådan reglering är tillåten framgår av det ovan sagda. Just syftet att bekämpa brott nämns särskilt i artikel 23.1 d. Frågan om den mottagande behöriga myndigheten har rätt att behandla uppgifterna avgörs av om det finns en rättslig grund för behandling i enlighet med det nya dataskyddsdirektivet (jfr 2 kap. 1 § brottsdatalogen).

³⁹ Jfr Fi2017/02899/S3 s. 56.

Utlämnande av personuppgifter

Frågor om utlämnande kan alltså, som beskrivits ovan, regleras av sekundära ändamålsbestämmelser. Många registerförfattningar innehåller därtill bestämmelser om utlämnande av personuppgifter vars syfte är att möjliggöra ett uppgiftsutbyte som annars skulle förhindras av sekretess. Uppgiftsskyldighet mellan svenska myndigheter bryter exempelvis eventuell sekretess och kan förekomma i registerförfattningar (10 kap. 28 § offentlighets- och sekretesslagen). När det gäller utländska myndigheter föreskrivs normalt sett inte uppgiftsskyldighet utan att uppgifter får lämnas ut under vissa förutsättningar. Sådana bestämmelser innebär också att sekretessbelagda uppgifter kan lämnas (8 kap. 3 § offentlighets- och sekretesslagen).⁴⁰

Även om sekretessbrytande bestämmelser inte i första hand reglerar förutsättningar för automatiserad personuppgiftsbehandling menar vi att de ändå får en sådan betydelse för personuppgiftsbehandlingen att de bör ingå i en bedömning av regleringens förenlighet med dataskyddsförordningen. Sekretessbrytande bestämmelser möjliggör nämligen utlämnanden som annars inte hade kunnat komma i fråga. Uppgiftsskyldighet för en myndighet som för ett automatiserat register som innehåller personuppgifter kommer därtill alltid innebära en automatiserad personuppgiftsbehandling för att kunna fullgöras.

Regler som syftar till att bryta sekretess får anses vara sådana preciseringar av principer om personuppgiftsbehandling som är tillåtna enligt artikel 6.2. Att automatiserat utlämnande kan regleras i nationell rätt har också stöd i artikel 6.3, där det nämns att den rättsliga grunden kan innehålla bestämmelser om till vilka ”enheter” personuppgifter får lämnas och för vilka ändamål. Även om sekretessbrytande bestämmelser inte är ändamålsbestämmelser i egentligen mening framgår ofta syftet med utlämnandet av bestämmelserna.⁴¹

Eftersom sekretessbrytande bestämmelser om utlämnande inte egentligen reglerar dataskyddsfrågor måste myndigheterna även ta

⁴⁰ Se exempelvis prop. 2009/10:85 s. 199 och 329.

⁴¹ Jfr SOU 2017:74 s. 324 f., SOU 2017:66 s. 309–311 och Ds 2017:28 s. 123–125. Jfr även SOU 2015:39 s. 283 f. avseende förhållandet mellan myndigheters uppgiftsskyldighet och finalitetsprincipen.

ställning till den dataskyddsrättsliga regleringen för att avgöra om en automatiserad personuppgiftsbehandling kan vidtas för att utlämna uppgifterna. När det gäller automatiserade överföringar till tredje land regleras exempelvis sådana både i gällande rätt och i dataskyddsförordningen. Även om ett uppgiftsutlämnande som omfattar personuppgifter till ett tredje land i och för sig kan ske utan hinder av sekretess, måste alltså en prövning göras av om gällande dataskyddsbestämmelser avseende tredjelandsöverföring m.m. medger att uppgiftslämnandet sker automatiserat.⁴²

Utlämnande för statistiska ändamål

Ibland regleras särskilt att uppgifter som behövs för statistik ska lämnas till en annan myndighet som ansvarar för sådan statistik. Att behandling för statistikändamål alltid ska anses förenlig med behandling för ursprungsändamålen framgår av artikel 5.1 b, om det sker i enlighet med artikel 89.1. I artikel 89.1 ställs särskilda krav på behandling för statistiska m.fl. ändamål. Att utlämnandet till myndigheter som har särskilda uppdrag att behandla statistik regleras i en registerförfattning får anses förenligt med dataskyddsförordningen.

Vilka uppgifter som får behandlas

Registerförfattningar kan föreskriva vilka personuppgifter som får behandlas. Detta kan göras rent allmänt genom en bestämmelse om att möjligheten att behandla personuppgifter gäller de personuppgifter som behövs för ett visst angivet ändamål. Mer precisa bestämmelser kan finnas i författningar som avser ett särskilt register, där en uppräknings ibland görs av de personuppgifter som ska ingå i registret (exempelvis namn, personnummer, adress etc).

I artikel 6.3 nämns uttryckligen att den rättsliga grunden kan innehålla bestämmelser om vilka uppgifter som får behandlas. Att föreskriva vilka uppgifter som får behandlas kan också uppfattas som en precisering som syftar till att följa principen om

⁴² Jfr prop. 2009/10:85 s. 202 f.

uppgiftsminimering i artikel 5.1 c och det följer därmed även av artikel 6.2 att nationell rätt kan innehålla sådana bestämmelser.⁴³

När det gäller mer renodlade register över personer är det givetvis ofta så att det föreskrivs att personnummer ska ingå i registret. Vi återkommer till reglering av användning av personnummer i det följande (avsnitt 2.5.5). Den särskilda regleringen av känsliga personuppgifter tar vi upp i avsnitt 2.5.6.

Elektroniskt utlämnande av personuppgifter m.m.

Registerförfattningar kan reglera vissa särskilda tekniska former av utlämnande, exempelvis s.k. *direktåtkomst*. Direktåtkomst är ett begrepp som kan sägas beskriva inte bara en teknisk lösning för att lämna ut uppgifter, utan också innebär ett utlämnande som får specifika rättsliga följder.⁴⁴

I artikel 6.3 nämns särskilt ”typer av behandling och förfaranden för behandling”. Nationella bestämmelser som preciserar förutsättningarna för elektroniskt utlämnande, inklusive direktåtkomst, får därmed anses förenliga med dataskyddsförordningen. Även andra bestämmelser som avser mer tekniska förfaranden med personuppgifter, exempelvis samkörning av register, får anses förenliga med dataskyddsförordningen i enlighet med artikel 6.3 i denna del.⁴⁵

Tillgång till personuppgifter inom myndigheten och sök begränsningar

I registerförfattningar, särskilt i informationshanteringsförfattningar, kan det finnas en reglering av den interna åtkomsten till personuppgifter, exempelvis vilka uppgifter som får göras *gemensamt tillgängliga*. Med detta begrepp brukar avses tillgänglighet för en vidare krets tjänstemän inom myndigheten. Andra begränsande bestämmelser kan vara att det anges att åtkomst till person-

⁴³ Jfr Fi 2017/02899/S3 s. 85 f.

⁴⁴ Se vidare SOU 2015:39 s. 136–141.

⁴⁵ Jfr Ds 2017:28 s. 125 och Fi 2017/02899/S3 s. 86 f. I SOU 2017:66 s. 287 f. och Ds 2017:41 s. 213 berörs frågan om skrivningen i skäl 31, som kan tolkas som att direktåtkomst inte skulle vara tillåten enligt dataskyddsförordningen. Utredningarna bedömer dock att skäl 31 inte kan uppfattas så, eller annars få till effekt att direktåtkomst inte skulle vara tillåten enligt dataskyddsförordningen. Vi delar denna bedömning.

uppgifter (både till gemensamt tillgängliga uppgifter eller uppgifter i ett specifikt register) för varje tjänsteman begränsas till vad som är nödvändigt för att han eller hon ska kunna fullgöra sin arbetsuppgift eller bestämmelser som reglerar behörigheter att ta del av personuppgifter.

En annan typ av reglering som kan sägas minska åtkomsten till personuppgifter är bestämmelser som begränsar sökmöjligheterna, exempelvis genom att ange att vissa sökbegrepp inte får användas.

Bestämmelser som på sådana sätt begränsar åtkomsten till personuppgifter får ses som preciseringar av principen om uppgiftsminimering (artikel 5.1 c). Man kan också se dem som en precisering av principen om integritet och konfidentialitet (artikel 5.1 f). De bör alltså betraktas som tillåtna kompletteringar i nationell rätt enligt artikel 6.2 dataskyddsförordningen.⁴⁶

Bevarande och gallring

Att personuppgifter inte får lagras i identifierbar form under längre tid än vad som är nödvändigt för de ändamål för vilka de behandlas är en grundläggande princip för behandling av personuppgifter enligt artikel 5.1 e. När det gäller bevarande för exempelvis arkivändamål anger samtidigt denna del av artikel 5.1 att sådant bevarande är tillåtet under förutsättning att bl.a. tekniska åtgärder säkerställer den registrerades rättigheter.

Gallringsbestämmelser kan ha formen av absoluta tidsgränser för när en uppgift ska tas bort eller när den inte längre får behandlas. Sådana bestämmelser får anses förenliga med dataskyddsförordningen, eftersom de preciserar principen om lagringstid i artikel 5.1 e. I artikel 6.3 i dataskyddsförordningen nämns också särskilt att lagringstid kan regleras i nationell rätt.

I samband med gallrings- eller bevarandebestämmelser kan också förekomma att regeringen eller den myndighet regeringen bestämmer ges rätt att meddela föreskrifter om bevarande eller gallring. Sådana bestämmelser är förenliga med dataskyddsförordningen, se även under nästa rubrik. Föreskrifter som i sig

⁴⁶ Jfr SOU 2017:66 s. 285–288, Ds 2017:28 s. 142–145, Fi 2017/02899/S3 s. 89 och Ds 2017:41 s. 143 f.

avser preciseringar av vad som gäller för bevarande för arkivändamål är förenliga med dataskyddsförordningen enligt vad som sagts ovan. Sådana föreskrifter bör också kunna ses som skyddsåtgärder som krävs enligt artikel 89.1.⁴⁷

Det kan också förekomma bestämmelser som mer allmänt anger att personuppgifter inte får bevaras, alternativt ska gallras, när de inte längre behövs för de ändamål de behandlas för. Sådana bestämmelser är snarlika vad som redan följer av artikel 5.1 e i dataskyddsförordningen. När det gäller bestämmelser som anger att *gallring* ska ske menar vi dock att sådana tillför något utöver dataskyddsförordningens allmänna princip. En uttrycklig gallringsbestämmelse får enligt svensk rätt till följd att personuppgifter får tas bort även om de ingår i allmänna handlingar.⁴⁸ Utan sådana bestämmelser gäller som utgångspunkt att allmänna handlingar, även sådana som innehåller personuppgifter, ska bevaras. Den allmänna principen i dataskyddsförordningen medger att personuppgifter bevaras för arkivändamål även efter det att det inte längre finns behov av att behandla dem för några andra ändamål. En uttrycklig gallringsbestämmelse, även om tidpunkten för gallring inte är bestämd i förväg, innebär alltså en precisering i förhållande till dataskyddsförordningen och kan därmed behållas med stöd av artikel 6.2 och 6.3.

Det kan förhålla sig annorlunda med bestämmelser som mer allmänt anger att *bevarande* av personuppgifter inte får ske, i en viss verksamhet eller i ett visst automatiserat system, om personuppgifterna inte behövs för vissa ändamål. När personuppgifter avskiljts från en viss verksamhet eller från ett visst behandlingssystem är utgångspunkten fortfarande att de ska bevaras, såvitt de ingår i allmänna handlingar.⁴⁹ När det gäller sådana bestämmelser kan man ifrågasätta om de tillför något utöver dataskyddsförordningens allmänna princip om lagringsminimering och om de därmed inte kan behållas i nationell rätt. Vi gör vidare överväganden om en sådan bestämmelse i avsnitt 4.1.4.

Utredningen om 2016 års dataskyddsdirektiv har föreslagit en viss förändring i gallringsbestämmelser i de registerförfattningar

⁴⁷ Jfr exempelvis SOU 2017:66 s. 295–298 och Ds 2017:28 s. 177–181.

⁴⁸ Jfr prop. 2011/12:45 s. 79.

⁴⁹ Se exempelvis prop. 2013/14:110 s. 502, jfr prop. 2009/10:85 s. 207 och 210.

som omfattas av utredningens uppdrag. Utredningen anser att begreppet *gallring* i huvudsak inte bör användas i bestämmelser som avser dataskydd.⁵⁰ Även Informationshanteringsutredningen har framfört liknande synpunkter på användningen av begreppet *gallring*.⁵¹ Dataskyddsförordningen hindrar inte att terminologin i detta avseende förändras i nationell rätt. Vi gör vidare överväganden i avsnitt 4.1.5, 5.5 och 6.5.

När det slutligen gäller behandling för arkivändamål anses sådan behandling, som vi noterat inledningsvis, tillåten enligt artikel 5.1 under förutsättning att bl.a. tekniska åtgärder säkerställer den registrerades rättigheter. Vi menar att frågor om arkivering och vilka krav som dataskyddsförordningen ställer på eventuell behandling av personuppgifter i samband med arkivering inte omfattas av vårt uppdrag. Den rättsliga grunden för att arkivera följer inte i första hand av de registerförfattningar som ingår i vårt uppdrag, utan av bestämmelserna i tryckfrihetsförordningen och arkivlagstiftningen.⁵² Vi gör bedömningen att förutsättningarna för myndigheternas bevarande av allmänna handlingar inte har förändrats genom att dataskyddsförordningen ska tillämpas i stället för personuppgiftslagen.⁵³

Bestämmelser om föreskriftsrätt m.m.

Registerförfattningar som är lagar ger ofta en rätt för regeringen eller den myndighet regeringen bestämmer att meddela föreskrifter i något eller flera avseenden som rör personuppgiftsbehandling, eller upplyser om att regeringen eller den myndighet regeringen bestämmer meddelar sådana föreskrifter. Vi bedömer att sådana bestämmelser inte berörs av dataskyddsförordningen.⁵⁴ Förordningen använder ofta uttryck som *nationell rätt* eller *bestämmelser*, se exempelvis artikel 6.2 eller 6.4. Som framgår av skäl 41 avses inte heller med uttrycket *rättslig grund* eller *lagstiftningsåtgärd* att det måste vara fråga om en lag antagen av ett nationellt parlament (jfr

⁵⁰ SOU 2017:74 s. 356–362.

⁵¹ SOU 2015:39 s. 546 f. Se även utredningens allmänna reflektioner om bevarande- och gallringsbestämmelser i registerförfattning, a. a. s. 539–541.

⁵² SOU 2017:39 s. 215 f.

⁵³ Jfr dock Ds 2017:41 s. 244–249.

⁵⁴ Jfr Ds 2017:33 s. 135.

avsnitt 2.5.2). Att frågor regleras i förordnings- eller föreskriftsform får alltså anses vara förenligt med dataskyddsförordningen.

Vi har för övrigt inte funnit någon anledning att inom ramen för vårt uppdrag överväga frågor om normgivningskompetens. Det kan dock anmärkas att regeringens restkompetens enligt 8 kap. 7 § regeringsformen torde omfatta reglering av personuppgiftsbehandling så länge inte 2 kap. 6 § regeringsformen innebär att regleringen måste ha lagform.⁵⁵

2.5.5 Personnummer

Enligt artikel 87 i dataskyddsförordningen får medlemsstaterna närmare bestämma på vilka särskilda villkor ett nationellt identifikationsnummer eller något annat vedertaget sätt för identifiering får behandlas. Om behandling av identifikationsnummer tillåts på angivna särskilda villkor, ställer artikeln upp ett krav på att identifikationsnumret ska användas med iakttagande av lämpliga skyddsåtgärder för den registrerades rättigheter och friheter enligt förordningen.

Dataskyddsutredningen föreslår en nationell bestämmelse som uppställer villkor för behandling av personuppgifter i 3 kap. 13 § dataskyddslagen. Uppgifter om personnummer eller samordningsnummer ska enligt bestämmelsen få behandlas utan samtycke endast när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl.

I några av de författningar som ingår i vårt uppdrag finns bestämmelser som anger att personnummer ska eller får användas i vissa sammanhang. Det är i viss mån tveksamt om en sådan reglering innebär ett *bestämmande av särskilda villkor* för användande i dataskyddsförordningens mening. Om det är fråga om ett sådant bestämmande av särskilda villkor ska skyddsåtgärder iakttas vid användandet. Om det inte är det, behöver någon bedömning av förekomsten av skyddsåtgärder inte göras.⁵⁶

⁵⁵ Jfr SOU 2017:39 s. 84.

⁵⁶ Jfr SOU 2017:66 s. 257, Fi2017/02899/S3 s. 117, Ds 2017:28 s. 173 och Ds 2017:19 s. 165–168.

I många fall torde man kunna se en författningsreglering som påbjuder eller tillåter användandet av personnummer som en redan gjord avvägning av samma förhållanden som kommer att vara styrande vid tillämpningen av 3 kap. 13 § dataskyddslagen (eller den likalydande bestämmelsen i 22 § personuppgiftslagen) – dvs. det ska vara klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl. En annan fråga är om en författningsreglering som kan sägas motsvara de krav dataskyddslagen ställer på behandling av personnummer, utan vidare kan anses uppfylla även dataskyddsförordningens krav på sådan behandling.⁵⁷

Trots att det kan diskuteras hur man ska se på dataskyddsförordningens krav i artikel 87 och på vilket sätt de kan anses uppfyllda, har vi valt att göra vissa överväganden kring vad som kan betraktas som skyddsåtgärder när det gäller de författningar som ingår i vårt uppdrag och som i någon mening reglerar användandet av personnummer. Dataskyddsutredningen menar att kravet i detta avseende inte kan vara särskilt högt ställt och att det torde finnas ett stort utrymme för medlemsstaterna att bestämma vilka skyddsåtgärder som behövs.⁵⁸

2.5.6 Känsliga personuppgifter

Behandlingen av särskilda kategorier personuppgifter är särskilt reglerad i artikel 9. Med *särskilda kategorier av uppgifter* avses bl.a. sådana som enligt personuppgiftslagen och andra registerförfattningar i dag brukar kallas *känsliga personuppgifter*, alltså uppgifter om ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening, hälsa eller sexualliv. Utöver dessa uppgifter gäller förordningens särskilda reglering för genetiska och biometriska uppgifter samt för uppgifter om sexuell läggning. I det följande används begreppet *känsliga personuppgifter* som beteckning för de uppgiftskategorier som räknas upp i dataskyddsförordningens artikel 9.1. En motsvarande särreglering gäller enligt det nya dataskyddsdirektivet

⁵⁷ Se även föregående not.

⁵⁸ SOU 2017:39 s. 199.

(artikel 10). Både Dataskyddsutredningen och Utredningen om 2016 års dataskyddsdirektiv föreslår att känsliga personuppgifter ska användas som begrepp för de uppgifter som avses med särregleringen i EU-rättsakterna (3 kap. 1 § dataskyddslagen och 2 kap. 13 § brottsdatalagen).

Utgångspunkten enligt artikel 9 är att behandling av känsliga personuppgifter är förbjuden. Från förbudet görs dock vissa undantag i artikel 9.2. Det undantag som i första hand blir aktuellt för personuppgiftsbehandlingen inom offentlig sektor är 9.2 g – behandlingen är nödvändig av hänsyn till ett viktigt allmänt intresse, på grundval av unionsrätten eller medlemsstaternas nationella rätt. Den nationella rätten ska i så fall uppfylla vissa krav, bl.a. ska den vara förenlig med det väsentliga innehållet i rätten till dataskydd.

Dataskyddsutredningen har närmare analyserat vilka krav som ställs för att göra undantag från dataskyddsförordningens förbud att behandla känsliga personuppgifter. Utredningen föreslår en generell reglering som gäller myndigheters behandling av känsliga personuppgifter i 3 kap. 3 § dataskyddslagen. Vidare föreslår utredningen en begränsning av sökmöjligheterna såvitt avser sådana personuppgifter (3 kap. 4 § dataskyddslagen). Som Dataskyddsutredningen påpekar innebär regleringen i dataskyddslagen att sektorsspecifika författningar ytterligare kan precisera och avgränsa möjligheterna att behandla känsliga personuppgifter. En reglering som ger utrymme för en behandling i större omfattning än de generellt tillämpliga bestämmelserna i dataskyddslagen är också tänkbar, givetvis under förutsättning att den är förenlig med dataskyddsförordningen. I vårt arbete har vi i första hand jämfört befintliga bestämmelser med dataskyddslagens reglering. Så länge en annan reglering ger uttryck för samma restriktivitet som dataskyddslagens anser vi att man kan utgå ifrån att den också är förenlig med dataskyddsförordningen.

2.5.7 Bestämmelser som inte kan behållas

Hänvisningar till personuppgiftslagen

I och med att personuppgiftslagen upphävs⁵⁹ måste bestämmelser som hänvisar till den lagen tas bort, antingen genom att paragrafer upphävs eller genom att de får ett nytt innehåll.

Som tidigare redogjorts för är en vanligt förekommande hänvisning till personuppgiftslagen en upplysande bestämmelse om att en registerförfattning gäller *utöver* personuppgiftslagen.

En annan vanligt förekommande hänvisning till personuppgiftslagen gäller bestämmelser om rättelse och skadestånd. Vi återkommer i avsnitt 2.5.9 till om det finns ett behov av att införa motsvarande hänvisningar till dataskyddsförordningen.

Skyldighet att utse personuppgiftsombud

Av registerförfattningar framgår ibland en skyldighet för den personuppgiftsansvarige att utse personuppgiftsombud.

I personuppgiftslagen definieras begreppet *personuppgiftsombud* (3 §). Att det finns ett personuppgiftsombud påverkar bl.a. anmälningsskyldigheten avseende behandling enligt 36 §. Bestämmelserna genomför 1995 års dataskyddsdirektiv.⁶⁰

I dataskyddsförordningen finns i stället bestämmelser om *dataskyddsombud* (artikel 37). Av förordningen framgår en direkt skyldighet att utse ett ombud om personuppgiftsbehandling genomförs av en myndighet eller ett offentligt organ (37.1 a). Eftersom förordningen är direkt tillämplig måste bestämmelser om personuppgiftsombud tas bort.

⁵⁹ SOU 2017:39 s. 49 (förslaget till dataskyddslag, ikraftträdande och övergångsbestämmelser p 2) och s. 78.

⁶⁰ Om bakgrunden till regleringen, se SOU 1997:39 s. 427 f. I 1995 års dataskyddsdirektivs svenska språkversion kallas ombudet för *uppgiftsskyddsombud*, men en annan terminologi föreslogs av Datalagskommittén (*persondataombud*) och sedan av regeringen (*personuppgiftsombud*), prop. 1997/98:44 s. 97 f.

2.5.8 Den enskildes rättigheter

Dataskyddsförordningens reglering av enskildas rättigheter

Dataskyddsförordningen innehåller bestämmelser om den enskildes rätt till rättelse (artikel 16), radering (artikel 17), begränsning av behandling (artikel 18) och rätt att göra invändningar mot behandling (artikel 21). Motsvarigheter till dessa rättigheter finns även upptagna i 1995 års dataskyddsdirektiv (artikel 12 b och artikel 14). Redan i dag har därför den enskilde enligt personuppgiftslagen rätt att få personuppgifter rättade, raderade eller blockerade om de behandlas i strid med personuppgiftslagen (28 §). Bestämmelsen genomför artikel 12 b i dataskyddsdirektivet. Artikel 14 i 1995 års dataskyddsdirektiv, rätten att göra invändningar, genomfördes däremot inte i personuppgiftslagen, utom såvitt avser rätten att invända mot direktreklam. Redan p.g.a. att det enligt gällande svensk rätt inte finns någon generell rätt att göra invändningar mot personuppgiftsbehandling innebär alltså dataskyddsförordningens reglering en nyhet. Man kan vidare övergripande konstatera att dataskyddsförordningens bestämmelser avseende enskildas rättigheter i vart fall är utförligare beskrivna än nuvarande bestämmelser i personuppgiftslagen och 1995 års dataskyddsdirektiv.⁶¹ Det finns därmed anledning att närmare analysera dataskyddsförordningens innebörd. Om förordningen innebär att den enskilde genom att åberopa sina rättigheter kan förhindra eller försvåra personuppgiftsbehandlingen vid någon myndighet finns nämligen anledning att överväga att utnyttja förordningens möjligheter till inskränkningar, som framgår av artikel 23. Samtidigt ska understrykas att den enskildes rättigheter fyller en viktig funktion ur rättsäkerhetssynpunkt. Det finns visserligen en risk för att effektiviteten i en myndighets arbete påverkas av om enskilda kan vända sig till myndigheten med olika krav. För att det ska kunna komma i fråga att begränsa den enskildes rättigheter i något avseende bör det dock vara fråga om att det finns en mer konkret risk för betydande effektivitetsförluster. Detta skulle kunna sägas framgå av artikel 23 och möjligheterna till begränsningar, som bl.a. anger att inskränkningar ska vara nödvändiga och proportionella i förhållande till syftet med inskränkningarna.⁶²

⁶¹ Jfr SOU 2017:66 s. 196 f.

⁶² Jfr Ds 2017:28 s. 167 f., Fi2017/02899/S3 s. 111 och SOU 2017:39 s. 207.

I det följande tar vi inte upp rätten till dataportabilitet (artikel 20), eftersom den gäller endast då personuppgifter behandlas på grund av samtycke eller avtal (se punkten a i artikel 20.1). Vi berör inte heller frågor om automatiserat beslutsfattande (artikel 22) eftersom artikeln inte innebär att den enskilde kan begära att någon viss åtgärd vidtas av den personuppgiftsansvariga myndigheten. Såvitt vi vet förekommer inte heller något automatiserat beslutsfattande inom ramen för verksamheten hos de myndigheter som berörs av vårt uppdrag.

Vi gör inte heller någon närmare analys av dataskyddsförordningens bestämmelser om information (artiklarna 13–15). Även om förordningens reglering är mer detaljerad, överensstämmer de grundläggande förutsättningarna för informationslämnande med den nuvarande ordningen enligt 23–26 §§ personuppgiftslagen. Det kan noteras att både artikel 13 och 14 innehåller en bestämmelse om undantag från informationskyldigheten avseende information som den registrerade redan förfogar över (jfr 25 § andra stycket personuppgiftslagen – information behöver inte lämnas om sådant som den registrerade redan känner till). Artikel 14 (14.5 b och c) innehåller också undantag för informationslämnande som skulle medföra en oproportionerlig ansträngning och då erhållande eller utlämnande av uppgifter uttryckligen föreskrivs i nationell rätt, under förutsättning att nationell rätt föreskriver lämpliga åtgärder för att skydda den registrerades berättigade intressen. Regleringen i denna del är jämförbar med 24 § personuppgiftslagen.

När det gäller informationslämnande gör vi dock överväganden avseende vissa specifika undantag från informationsplikten som i dag finns i kustbevakningsdatalagen, se vidare avsnitt 3.5.6.

Slutligen kan nämnas att den enskilde också har rätt till information om personuppgiftsincidenter enligt artikel 34, en rättighet som i och för sig är möjlig att inskränka enligt artikel 23. Vi har inte sett några skäl till inskränkningar som särskilt hänförs sig till de verksamheter som berörs av vårt uppdrag.⁶³ Redan av artikeln framgår att informationsplikten är begränsad på olika sätt, bl.a. inträder informationsplikt först vid ”höga risker” för enskildas rättigheter och den behöver heller inte fullgöras om tekniska eller

⁶³ Jfr den bedömning som görs i Ds 2017:41 s. 194 f.

organisatoriska åtgärder redan genomförts av den personuppgiftsansvarige. Om det blir aktuellt att lämna information om personuppgiftsincidenter torde sådan information kunna utformas så att sekretessbelagda uppgifter inte lämnas ut (se t.ex. 18 kap. 8 § offentlighets- och sekretesslagen)

Rättelse och komplettering (artikel 16)

De flesta registerförfattningar hänvisar i dag till skyldigheten enligt personuppgiftslagen att rätta personuppgifter på begäran av den enskilde. Samma rättighet framgår av den första meningen i artikel 16. Denna rättighet innebär alltså inte någon förändring i förhållande till gällande rätt och det finns ingen anledning att inom ramen för vår utredning överväga om det finns skäl att göra inskränkningar i den.⁶⁴

Artikel 16 innehåller också en nyhet genom att den föreskriver en rätt för den enskilde att få ofullständiga personuppgifter kompletterade ”bland annat genom att tillhandahålla ett kompletterande utlåtande”. Rättigheten ska utövas ”med beaktande av ändamålet med behandlingen”. En motsvarande rättighet finns i det nya dataskyddsdirektivet.⁶⁵ Som Utredningen om 2016 års dataskyddsdirektiv påpekar är det i viss mån oklart hur denna rättighet ska tolkas. Som utredningen anför följer det redan av förvaltningslagen att en enskild har rätt att ge in en skrivelse till en myndighet och där utveckla exempelvis skälen för en begäran. Utredningen anser att svensk rätt alltså redan kan anses uppfylla de EU-rättsliga kraven i denna del.⁶⁶ Vi anser att det är rimligt att tolka bestämmelsen i dataskyddsförordningen på samma sätt som Utredningen om 2016 års dataskyddsdirektiv tolkar den motsvarande bestämmelsen i det nya dataskyddsdirektivet. Som ett tillägg

⁶⁴ Eftersom dataskyddsförordningen inte uttrycker rättigheten annorlunda än 1995 års dataskyddsdirektiv bör innebörden av rättigheten kunna tolkas i enlighet med den nuvarande rätten till rättelse, se exempelvis SOU 2015:39 s. 569. Rättigheten motsvaras också av artikel 16.1 i det nya dataskyddsdirektivet som kommer att genomföras i brottsdatalogen. Den närmare innebörden behandlas i SOU: 2017:29 s. 403 f.

⁶⁵ I de svenska språkversionerna av direktivet respektive förordningen används olika uttrycksätt i artiklarna – *kompletterande utlåtande* i förordningen och *kompletterande inlägga* i direktivet. Det torde inte finnas någon skillnad i betydelse, eftersom den engelska språkversionen använder samma uttryck i båda rättsakterna – *supplementary statement*.

⁶⁶ SOU 2017:29 s. 404.

anser vi att rätten till komplettering inte kan uppfattas som en möjlighet för en enskild att komplettera uppgifter genom att *tillföra* uppgifter till ett författningsreglerat register. Om det i författningen regleras vilka uppgifter registret ska innehålla och uppgifterna om den registrerade inte är ofullständiga i förhållande till författningens krav, innebär alltså inte artikel 16 någon rätt för den registrerade att föra in ytterligare uppgifter i registret. I sådana fall är omfattningen av vilka personuppgifter som ska behandlas redan övervägd med beaktande av ändamålet med behandlingen. Oavsett detta kan givetvis den registrerade ge in ett utlåtande till myndigheten med sina synpunkter på den aktuella behandlingen.

Rätten till radering (artikel 17)

Även rätten till radering finns enligt gällande rätt genom 28 § personuppgiftslagen – uttrycket *utplåning* i den bestämmelsen får anses innebära samma sak som *radering*.

Artikel 17 anger dock, till skillnad från 28 § personuppgiftslagen och det bakomliggande dataskyddsdirektivet (artikel 12 b), på ett utförligt sätt i vilka situationer den enskilde har rätt till radering. Samtidigt finns ett undantag från rätten till radering i artikel 17.3 som anger att punkten 1 (och 2) inte ska gälla i den utsträckning behandlingen är nödvändig för att bl.a. uppfylla en rättslig förpliktelse i enlighet med medlemsstaternas nationella rätt eller för att utföra en uppgift av allmänt intresse eller vid myndighetsutövning. De grunder för behandling som anges i artikel 17.3 är alltså desamma som gör en behandling laglig i enlighet med artikel 6.1 c eller e. Med andra ord kan den registrerade inte framtvinga utplåning av personuppgifter som behövs för myndigheternas författningsreglerade verksamhet. Det kan tilläggas att behandling av personuppgifter som behövs för diarieföring eller för bevarande av allmänna handlingar alltid bör kunna betraktas som laglig med hänvisning till ett allmänt intresse, även om sådan behandling inte alltid behövs för myndighetens kärnverksamhet och därmed inte omfattas av någon författningsreglering som gäller specifikt för den aktuella myndigheten.

Vi anser alltså inte att det finns några skäl att inom ramen för vår utredning föreslå några inskränkningar i rätten till radering

enligt artikel 17. Det ska poängteras att detta inte står i någon motsättning till att skyldigheten att rätta personuppgifter ibland kan innebära att personuppgifter måste raderas från en viss informationssamling, exempelvis från ett register.⁶⁷

Begränsning av behandling (artikel 18)

Rätten att få behandlingen av personuppgifter begränsad följer av artikel 18. Begreppet *begränsning* definieras i artikel 4.3 som en ”markering av lagrade personuppgifter med syftet att begränsa behandlingen av dessa i framtiden”.

Dagens motsvarighet till begränsning är *blockering* enligt 28 § personuppgiftslagen. Den begränsning av behandling som avses med blockering är dock endast att personuppgifterna inte ska lämnas ut till tredje man. Av artikel 18.2 följer att begränsning i princip innebär att behandling av personuppgifterna utöver lagring inte längre får ske, utom i vissa undantagsfall.⁶⁸ Rätten till begränsning är alltså inte helt jämförbar med rätten till blockering enligt gällande rätt.

Enligt artikel 18.1 finns det olika förutsättningar under vilka den registrerade har rätt att kräva begränsning av behandlingen. En av dem (punkten b) är att behandlingen är olaglig, men att den registrerade motsätter sig att uppgifterna raderas. En behandling av personuppgifter som är olaglig måste under alla förhållanden upphöra, i vart fall behandling utöver att uppgifterna i någon form bevaras, exempelvis därför att de behandlade uppgifterna förekommer i allmänna handlingar.⁶⁹ Begränsning utesluter dock inte, som nämnts, att uppgifterna bevaras. Rätten till begränsning i samband

⁶⁷ Jfr SOU 2017:29 s. 405 och den däri gjorda hänvisningen till JO 2007/08 s. 67.

⁶⁸ Definitionen av begreppet *begränsning* görs på samma sätt i det nya dataskyddsdirektivet som i dataskyddsförordningen. Som Utredningen om 2016 års dataskyddsdirektiv anför framstår definitionen av begreppet som missvisande, bl.a. med beaktande av direktivets skäl 47 (SOU 2017:29 s. 409). Begränsning av behandling tas upp även i skälen till dataskyddsförordningen (skäl 67) på samma sätt som i direktivets skäl 47. Utformningen av artikel 18.2 i förordningen, som inte har någon motsvarighet i direktivet, klargör ytterligare att begränsning måste vara en åtgärd som rent faktiskt gör att personuppgifterna inte behandlas vidare, oavsett hur detta åstadkoms.

⁶⁹ Ett exempel som ges av Utredningen om 2016 års dataskyddsdirektiv är tillvägagångssättet när det gällde polisens s.k. kringresanderegister – det olagliga registret togs bort, men två kopior sparades bl.a. för att kunna användas som bevisning (SOU 2017:29 s. 410 och vidare SOU 2015:39 s. 574 f. och 645 f.)

med olaglig behandling behöver alltså inte inskränkas som vi ser det.

En annan situation då behandlingen ska begränsas är om den personuppgiftsansvarige inte längre behöver personuppgifterna för behandling, men den registrerade behöver dem bl.a. för att göra gällande rättsliga anspråk (punkten c). Även i en sådan situation framstår det som självklart att behandlingen ska begränsas – det är ju inte lagligt att fortsätta behandla personuppgifter om det inte finns ett godtagbart ändamål med behandlingen. Att göra någon generell inskränkning i den registrerade rätt till begränsning av behandlingen i en sådan situation framstår därmed inte heller som befogat.

En tredje förutsättning för begränsning av behandlingen är att den registrerade bestrider uppgifternas korrekthet och den personuppgiftsansvarige behöver tid att kontrollera deras riktighet. Vi anser inte att begränsningskravet i en sådan situation generellt kan sägas innebära en sådan olägenhet i en myndighets verksamhet att rättigheten behöver inskränkas. Det framstår som tämligen självklart att en myndighet kontrollerar uppgifters korrekthet oavsett om det är den enskilde själv eller någon annan som framför omständigheter som tyder på att uppgifterna inte stämmer. Detta följer inte minst av den personuppgiftsansvariges allmänna skyldighet att se till att personuppgifter är korrekta. Att behandlingen av uppgifterna, utöver att de bevaras, inte fortsätter under den tid det tar att fastställa riktigheten framstår även det som självklart. Det kan noteras att skyldigheten att begränsa behandlingen av personuppgifter inom det nya dataskyddsdirektivets tillämpningsområde (se artikel 16.3 i direktivet) kommer att gälla under i princip samma förutsättningar som enligt dataskyddsförordningens artikel 18.1 a och c och att det enligt direktivet inte finns några möjligheter att inskränka den personuppgiftsansvariges skyldigheter i det avseendet.⁷⁰

Slutligen ska behandlingen begränsas om den registrerade har invänt mot behandling i enlighet med artikel 21.1. Vi återkommer i

⁷⁰ Angående vad som är en *korrekt* uppgift, jfr SOU 2017:29 s. 258. Särskilt att märka är att personuppgifter som hänför sig till någons subjektiva uppfattning om något (exempelvis en förhørsutsaga) inte är oriktiga av det skälet att någon annan hävdar att de inte överensstämmer med verkligheten, inte ens om de rent faktiskt inte överensstämmer med verkligheten. Korrektheten har i sådana fall att göra med att utsagan återges på korrekt sätt.

nästa stycke till den närmare innebörden av artikel 21.1. Personuppgiftsbehandlingen ska begränsas under den tid det tar för den personuppgiftsansvarige att visa att förutsättningar att upphöra med behandlingen p.g.a. den registrerade invändning inte föreligger. Eftersom vi inte ser något generellt behov att inskränka rätten till invändningar enligt artikel 21.1 anser vi inte heller att rätten till begränsning bör inskränkas i det avseendet.

Det ska också noteras att det enligt artikel 18.2 finns möjligheter att fortsätta att behandla uppgifter trots att förutsättningarna för begränsning föreligger, om det sker av skäl som rör ett *viktigt allmänintresse* i en medlemsstat. Vi har tidigare diskuterat om det som avses med *viktigt* allmänintresse kan antas skilja sig från vad som avses med *allmänt intresse*, uttryckssättet som används i artikel 6.1 e. Samma frågeställning aktualiseras när det gäller artikel 18.2. Vi hänvisar återigen till Dataskyddsutredningens bedömning att det får anses vara ett viktigt allmänt intresse att svenska myndigheter kan bedriva den verksamhet som tydligt faller inom ramen för deras uppdrag på ett korrekt, rättssäkert och effektivt sätt.⁷¹ Med en sådan utgångspunkt torde det finnas tämligen långtgående möjligheter att fortsätta behandla personuppgifter trots att behandlingen ska begränsas. Under alla förhållanden menar vi att myndighetens skyldigheter enligt tryckfrihetsförordningen måste anses vara viktiga allmänna intressen och att myndigheten måste kunna behandla personuppgifter för att exempelvis lämna ut allmänna handlingar även om personuppgiftsbehandlingen i övrigt ska begränsas.

Rätt att göra invändningar (artikel 21)

Enligt artikel 21 har den enskilde rätt att när som helst göra invändningar mot personuppgiftsbehandling som grundar sig på artikel 6.1 e eller f. Om en myndighet alltså har en rättslig förpliktelse (artikel 6.1 c) att föra exempelvis ett visst register, gäller inte rätten till invändningar enligt artikel 21.

Om den personuppgiftsansvarige, efter invändning från den registrerade, inte kan visa på tvingande berättigade skäl för

⁷¹ SOU 2017:39 s. 173 f.

behandlingen som väger tyngre än den registrerades intressen, rättigheter och friheter eller om det sker för fastställande, utövande eller försvar av rättsliga anspråk, får den personuppgiftsansvarige inte längre behandla personuppgifter avseende den registrerade. Som det får förstås ska den registrerades intressen etc. hänföra sig till den registrerades egen ”specifika situation” i enlighet med uttryckssättet i artikelns inledande mening. Som nämnts är artikel 21 kopplad till artikel 18 på så sätt att personuppgiftsbehandlingen också ska begränsas under den tid som behövs för att den personuppgiftsansvarige ska kunna kontrollera om det finns berättigade skäl att fortsätta behandlingen (artikel 18.1 d).

Rätten till invändningar har en motsvarighet i 1995 års data-skyddsdirektiv, artikel 14, som också ger den registrerade rätt att göra invändningar och anger att personuppgiftsbehandlingen ska upphöra om skälen för invändningen är berättigade. Denna rättighet gäller dock endast om nationell rätt inte föreskriver något annat. Den generella rätten till invändningar genomfördes därför inte i personuppgiftslagen, utan i stället följer av 12 § andra stycket att den registrerade inte har rätt att invända mot behandling som är tillåten enligt lagen, utom i de fall då behandlingen grundar sig på samtycke (12 § första stycket) eller rör direkt marknadsföring (11 §).⁷²

Rent allmänt finns det givetvis skäl för att personuppgiftsbehandling vid en myndighet ska kunna fortgå även om den enskilde gör invändningar mot den. Artikel 21 innebär dock inget annat än att behandlingen också kan fortsätta, om inte den registrerades *berättigade* intressen av att behandlingen upphör väger tyngre än skälen för behandling. Det är svårt att avgöra på förhand i vilka fall ett berättigat intresse kan väga tyngre än allmänintresset av att personuppgiftsbehandlingen får fortgå. Möjligheten att göra invändningar kan innebära att en extra kontroll behövs av om personuppgiftsbehandlingen sker på ett lagligt och korrekt sätt och i övrigt verkligen behövs i det enskilda fallet. För invändningar som är helt obefogade torde det i många fall vara tillräckligt att hänvisa till de författningar som ger stöd för personuppgiftsbehandlingen för att det ska anses visat att intresset av behandling väger tyngre.

⁷² Se vidare prop. 1997/98:44 s. 122 f. och 65.

Inom ramen för vårt uppdrag ser vi därmed inga generella skäl att göra inskränkningar i rätten att göra invändningar enligt artikel 21.

Sammanfattning

Den enskildes rättigheter enligt dataskyddsförordningen innebär alltså sammanfattningsvis att den enskilde får i viss mån utökade möjligheter att invända mot behandling och få behandling begränsad, i vart fall under viss tid. Vi kan inte se att den enskildes möjligheter i dessa avseenden förhindrar sådan personuppgiftsbehandling som är laglig och som behövs för att myndigheter ska kunna bedriva sin verksamhet. Att den enskilde ges vissa utökade rättigheter kan givetvis i några fall leda till att enskilda gör invändningar eller begär begränsning av behandling som senare visar sig vara obefogade. Enbart av det skälet finns det inte anledning att göra inskränkningar i den enskildes rättigheter, och det torde heller inte vara möjligt, eftersom inskränkningar endast kan vidtas under de förutsättningar som anges i artikel 23.

2.5.9 Behovet av nya bestämmelser

Statiska eller dynamiska hänvisningar till dataskyddsförordningen?

För att en registerförfattning ska kunna tillämpas tillsammans med dataskyddsförordningen behövs i vissa fall hänvisningar till förordningens artiklar. En fråga som då ska övervägas är om hänvisningar ska göras till dataskyddsförordningen i den lydelse den har vid en viss tidpunkt (statiska hänvisningar) eller om hänvisningar ska avse dataskyddsförordningens vid varje tidpunkt gällande lydelse (dynamiska hänvisningar).

De bestämmelser vi föreslår som hänvisar till dataskyddsförordningen är av upplysande karaktär eller så begränsar eller preciserar de förordningens tillämpning på något område. Eftersom förordningen är direkt tillämplig finns det inga möjligheter för svenska myndigheter att i praktiken tillämpa en äldre lydelse av förordningen. Dynamiska hänvisningar i bestämmelser som har ett materiellt innehåll får visserligen ses över om innehållet i dataskyddsförordningen ändras. Genom en dynamisk hänvisnings-

teknik behöver dock lagstiftningen inte ändras om inte den förändrade lydelsen av förordningen också innebär någon förändring i sak.⁷³ Det kan tilläggas att även om förordningen ändras i sak är det inte säkert att det finns något utrymme för att precisera eller begränsa dess tillämpning på något annat sätt än som redan gjorts. Även i sådana fall kan man med dynamiska hänvisningar undvika att göra lagändringar endast av formella skäl. Vi använder oss alltså i samtliga fall av en dynamisk hänvisningsteknik. Det kan tilläggas att även Dataskyddsutredningen i huvudsak använder sig av dynamiska hänvisningar, liksom flera andra utredningar som behandlar anpassningar till dataskyddsförordningen.⁷⁴

Upplysande bestämmelse om dataskyddsförordningen

Som tidigare nämnts innehåller en hel del registerförfattningar i dag en bestämmelse som anger att registerförfattningen gäller utöver personuppgiftslagen. Syftet med sådana bestämmelser är att upplysa om den övergripande lagstiftningen. Även om det inte uttryckligen anges i en registerförfattning kommer personuppgiftslagen att vara tillämplig, så länge inte registerförfattningen innehåller en avvikande reglering. I och med EU:s dataskyddsreform kommer det att vara antingen dataskyddsförordningen eller brottsdatalagen som ska tillämpas som det generella regelverket, beroende på vilket tillämpningsområde en viss sorts behandling omfattas av. Behovet av en upplysande bestämmelse om vilken övergripande reglering som är tillämplig har alltså snarast ökat i och med reformen. Flertalet andra utredningar har konstaterat att det finns ett behov att införa en bestämmelse om att en registerförfattning kompletterar dataskyddsförordningen. Vi delar i huvudsak den bedömningen. I vissa fall framstår dock en upplysande bestämmelse som överflödigt. Det gäller författningar som i dag inte innehåller någon upplysande bestämmelse om förhållandet till personuppgiftslagen. För vissa författningar som ingår i vårt uppdrag gäller dessutom att de inte i första hand reglerar personuppgiftsbehandling, utan andra frågor. Den personuppgifts-

⁷³ Jfr prop. 2015/16:156 s. 34.

⁷⁴ SOU 2017:39 s. 80–82 och jfr exempelvis Ds 2017:19 s. 104, Fi2017/02899/S3 s. 63 och Ds 2017:26 s. 36.

behandling som kan bli aktuell till följd av sådana författningar framstår också ofta som mindre omfattande och väl avgränsad. Det skulle därmed endast tynga författningstexten att införa upplysande bestämmelser, som dessutom skulle ha ett begränsat värde för tillämparen.

Bestämmelser om förhållandet till dataskyddslagen

När det gäller förhållandet till dataskyddslagen föreslår vidare flertalet utredningar att denna lag också tas upp i en upplysande bestämmelse gällande dataskyddsförordningen. Eftersom dataskyddslagen kommer att innehålla bestämmelser som mer generellt kompletterar dataskyddsförordningen menar även vi att en upplysande bestämmelse som hänvisar till dataskyddsförordningen bör ta upp dataskyddslagen.

Dataskyddslagen innehåller de generella bestämmelser som Dataskyddsutredningen ansett vara nödvändiga och lämpliga för att komplettera dataskyddsförordningen i svensk rätt. Den riktar sig inte endast till myndigheter. En del bestämmelser i dataskyddslagen kommer inte att vara aktuella att tillämpa för vissa myndigheter, beroende på vilken verksamhet som ingår i deras uppdrag. Myndigheternas registerförfattningar kan också komma att innehålla avvikande bestämmelser, exempelvis om känsliga personuppgifter. När det gäller förhållandet till dataskyddslagen hade man därmed kunnat tänka sig en reglering som utgår ifrån att en viss registerförfattning gäller *i stället för* dataskyddslagen, om inte vissa bestämmelser uttryckligen anges som tillämpliga. Denna teknik har använts avseende personuppgiftslagens tillämplighet, framför allt i registerförfattningar som reglerar personuppgiftsbehandlingen hos brottsbekämpande myndigheter. En fördel med denna lagtekniska lösning har ansetts vara att den är tydligare och underlättar för tillämparen.⁷⁵ En viss ökad tydlighet skulle visserligen kunna uppnås med att välja en liknande teknik beträffande registerförfattningars förhållande till dataskyddslagen. Samtidigt utgör dataskyddslagen endast en begränsad del av den övergripande

⁷⁵ Se exempelvis prop. 2004/05:164 s. 47 f., prop. 2009/10 :85 s. 80 f. och prop. 2011/12 :45 s. 76 f.

reglering som myndigheterna måste tillämpa framöver, eftersom dataskyddsförordningen samtidigt är direkt tillämplig. Att låta en registerförfattning gälla i stället för dataskyddslagen innebär därtill ett behov av att se över registerförfattningen varje gång dataskyddslagen ändras, så att inte hänvisningarna blir felaktiga eller missvisande.⁷⁶ Vi har därför stannat för att inte använda en sådan lagstiftningsteknik, utan föreslår hänvisningar som upplyser om att dataskyddslagen gäller, om inte något annat följer av den aktuella registerförfattningen eller föreskrifter meddelade med stöd av den. När det gäller lagen (2000:344) om Schengens informationssystem har vi dock gjort en till viss del annan bedömning, se vidare avsnitt 7.4.

Tillsyn

Bestämmelser om tillsyn finns i dag i personuppgiftslagen. När dataskyddsförordningen ska börja tillämpas kommer tillsynsbestämmelser att finnas i förordningen i stället. Av 6 kap. 1 § dataskyddslagen kommer därtill att framgå att tillsynsmyndigheten har befogenheter som avser både efterlevnaden av dataskyddslagen och andra författningar som kompletterar dataskyddsförordningen. I 6 kap. dataskyddslagen finns vissa andra bestämmelser som Dataskyddsutredningen föreslår som komplement till dataskyddsförordningen och som avser tillsyn. Vi bedömer att det inte finns något behov av några ytterligare hänvisningar eller bestämmelser som avser tillsyn än vad som föreslås av Dataskyddsutredningen.⁷⁷

Skadestånd och rättsmedel

Av 8 kap. 1 § dataskyddslagen framgår att rätten till skadestånd enligt dataskyddsförordningen också gäller vid överträdelse av dataskyddslagen och andra författningar som kompletterar dataskyddsförordningen. Det behövs alltså inga hänvisningar till dataskyddsförordningen avseende skadestånd i registerförfattningar som kompletterar förordningen (jfr motsatsvis dagens

⁷⁶ Jfr Lagrådets kritik av ”i stället för”-tekniken i prop. 2000/01:33 s. 345 f.

⁷⁷ Jfr Ds 2017:26 s. 62 f., Fi2017/02899/S3 s. 124 och SOU 2017:66 s. 298 f.

hänvisningar till personuppgiftslagen, som dock beror på att skadestånd i enlighet med bestämmelsen där endast gäller för behandling ”enligt denna lag”).⁷⁸

Beslut om rättelse m.m. avseende personuppgiftsbehandling enligt en registerförfattning kommer att fattas med direkt tillämpning av dataskyddsförordningen. Sådana beslut kommer därmed att kunna överklagas med stöd av 8 kap. 2 § dataskyddslagen. Det finns alltså inget behov att införa några bestämmelser om överklagande i registerförfattningar, i vart fall inte i dem som omfattas av vårt uppdrag.⁷⁹

Sanktionsavgifter

Enligt artikel 83 i dataskyddsförordningen får tillsynsmyndigheten fatta beslut om sanktionsavgifter. Även myndigheter föreslås kunna bli skyldiga att betala sanktionsavgifter enligt 7 kap. 1 § dataskyddslagen.

Av artikel 83.5 b följer att sanktionsavgifter kommer att kunna åläggas om den enskildes rättigheter enligt artikel 12–22 åsidosatts. Dessa artiklar kommer att tillämpas direkt av myndigheterna och sanktionsavgifter kan alltså komma ifråga i sådana fall även utan att någon hänvisning görs till dataskyddsförordningen eller dataskyddslagen.

Av artikel 83.5 a följer att sanktionsavgift ska kunna åläggas om en personuppgiftsansvarig bryter mot grundläggande principer för behandling enligt, såvitt nu är av intresse, artiklarna 5, 6 och 9. Vi menar att överträdelse av bestämmelser i en registerförfattning i många fall bör kunna ses även som en överträdelse av artiklarna 5, 6 och 9. Många bestämmelser i registerförfattningar får, som vi redan utvecklat, ses som preciseringar av de allmänna principerna för personuppgiftsbehandling enligt artikel 5. Personuppgiftsbehandling som inte har stöd i den aktuella registerförfattningen torde inte heller ha stöd i någon annan författning som kan utgöra rättslig grund för behandlingen, och sådan behandling torde då också strida mot artikel 6. Behandling av känsliga personuppgifter i strid

⁷⁸ Jfr exempelvis Ds 2017:28 s. 184, Ds 2017:19 s. 157, Fi2017/02899/S3 s. 119, SOU 2017:66 s. 302.

⁷⁹ Jfr Ds 2017:28 s. 183, Fi2017/02899/S3 s. 129, SOU 2017:66 s. 306–309.

med en bestämmelse i en registerförfattning har inte det stöd i nationell rätt som krävs för att behandling ska få ske trots det grundläggande förbudet i förordningens artikel 9. Sammanfattningsvis torde alltså överträdelser av en registerförfattnings bestämmelser i de flesta fall kunna betraktas som en överträdelse även av dataskyddsförordningen och därmed föranleda sanktionsavgift. Det finns enligt vår mening ingen anledning att förtydliga eller hänvisa till detta förhållande, i vart fall inte i de registerförfattningar som ingår i vårt uppdrag.⁸⁰

2.6 Allmänna överväganden om anpassningen av registerförfattningar till det nya dataskyddsdirektivet

2.6.1 Rättslig grund för personuppgiftsbehandlingen

Enligt artikel 8.1 i det nya dataskyddsdirektivet är behandling av personuppgifter laglig endast om behandlingen är nödvändig för att en behörig myndighet ska kunna utföra en uppgift på grundval av unionsrätt eller nationell rätt för de syften som också omfattas av direktivets allmänna tillämpningsområde, dvs. bekämpa brott m.m. Artikel 8.1 genomförs på generell nivå genom 2 kap. 1 § brottsdatalagen. Av bestämmelsen framgår vidare att arbetsuppgiften i fråga ska framgå av en bindande unionsrättsakt, av en lag, en förordning eller ett särskilt beslut i vilket regeringen uppdragit åt en behörig myndighet att ansvara för en sådan uppgift. Utredningen om 2016 års dataskyddsdirektiv anför följande om kravet på rättslig grund.

En myndighets arbetsuppgifter styrs i huvudsak av dess instruktion, medan vilken personuppgiftsbehandling som kan aktualiseras inom ramlagens tillämpningsområde styrs av de materiella bestämmelserna för verksamheten. Inom ramlagens tillämpningsområde rör det sig framför allt om reglerna om utredning av brott, brott-målsprocess och straffverkställighet. Genom de författningar som reglerar den verksamhet i vilken personuppgifterna behandlas, tillsammans med ramlagen och registerförfattningarna, är enligt utredningens mening kravet

⁸⁰ Jfr SOU 2017:66 s. 302–305 och Fi2017/02899/S3 s. 127.

i direktivet på att behandlingen ska ha stöd i unionsrätt eller nationell rätt uppfyllt.⁸¹

Av de författningar som ingår i vårt uppdrag och som faller inom det nya dataskyddsdirektivets tillämpningsområde framgår att de inte bara innebär en särreglering av personuppgiftsbehandling, utan också ålägger Polismyndigheten en specifik uppgift att behandla vissa personuppgifter. När det gäller begreppet nödvändig gör Utredningen om 2016 års dataskyddsdirektiv i huvudsak samma bedömning som Dataskyddsutredningen – kravet är alltså inte så långtgående som att det ska vara omöjligt att utföra den aktuella uppgiften utan att behandla personuppgifter, utan det räcker att man kan konstatera att personuppgiftsbehandling behövs.⁸²

Vi återkommer kort till frågan om rättslig grund i avsnitt 5.3, 6.3 och 7.3.1.

2.6.2 Övergripande om möjligheten att införa och behålla särreglering

Ett direktiv innebär en skyldighet för medlemsstaterna att införa föreskrifter i överensstämmelse med direktivet. Medlemsstaterna är dock fria att bestämma form och tillvägagångssätt för genomförandet. Detta innebär att medlemsstaterna inte är bundna av t.ex. ett direktivs terminologi och systematik, om väl det avsedda resultatet uppnås med en annan terminologi och systematik. Avgörande är att lagstiftningen uppnår det resultat i sak som direktivet eftersträvar. Det framgår vidare av det nya dataskyddsdirektivet att det är ett minimidirektiv, dvs. det finns möjligheter för medlemsstaterna att införa starkare skyddsåtgärder för den enskildes rättigheter och friheter med avseende på personuppgiftsbehandling inom direktivets tillämpningsområde (artikel 1.3).

Det nya dataskyddsdirektivet innehåller i artikel 4 principer för personuppgiftsbehandling som i huvudsak överensstämmer med dataskyddsförordningens artikel 5, 1995 års dataskyddsdirektiv och därmed med personuppgiftslagen. Många bestämmelser i registerförfattningar kan, som redan behandlats i avsnitt 2.5.4 ses som

⁸¹ SOU 2017:29 s. 238.

⁸² A. a. s. 237.

preciseringar av dessa grundläggande principer och är därmed förenliga med det nya dataskyddsdirektivet likväl som med dataskyddsförordningen. Att det är förutsatt att nationell rätt kommer att innehålla specificeringar i förhållande till direktivet kan därtill sägas framgå av artikel 8.2 – bestämmelsen anger att medlemsstaternas nationella rätt som reglerar behandling enligt direktivet *åtminstone* ska specificera syftet med behandlingen, vilka personuppgifter som ska behandlas och behandlingens ändamål.

På direktivets område kommer brottsdatalagen bli den grundläggande regleringen av personuppgiftsbehandling. I lagen har tagits in de bestämmelser som krävs för att genomföra direktivet, men också andra bestämmelser som motsvarar vad som i dag föreskrivs i skilda registerförfattningar inom direktivets tillämpningsområde. Utredningen om 2016 års dataskyddsdirektiv har gjort bedömningen att dessa bestämmelser är förenliga med direktivet. Utredningen har vidare bedömt att flertalet andra bestämmelser i nuvarande registerlagar är förenliga med direktivet och att förändringar därför inte behöver göras för att uppfylla direktivets krav, men däremot för att skapa en sammanhållen och fungerande reglering med hänsyn till införandet av brottsdatalagen.⁸³ Direktivet ställer dock i sig inga krav på att genomförandet ska ske endast i en lag eller liknande. En artikel i direktivet kan alltså genomföras i flera författningar om det skulle anses lämpligt i en medlemsstat.

2.6.3 Bestämmelser som är förenliga med direktivet

Syfte och tillämpningsområde

Utredningen om 2016 års dataskyddsdirektiv har föreslagit en bestämmelse om syfte i brottsdatalagen (1 kap. 1 §). Liknande bestämmelser i registerförfattningar kan alltså inte anses strida mot direktivet.

När det gäller tillämpningsområde blir det naturligen så att detta måste utgå från samma tillämpningsområde som direktivet har (jfr 1 kap. 2 § brottsdatalagen). Detta hindrar dock inte att tillämpningsområdet för en viss registerförfattning avgränsas ytterligare

⁸³ SOU 2017:74 s. 319.

exempelvis till att avse endast en viss myndighets verksamhet, en viss avgränsad informationssamling, exempelvis ett register, eller en viss behandlingssituation, exempelvis ett visst informationsutbyte.⁸⁴

Personuppgiftsansvar

Av artikel 3.8 framgår att om ändamålen med och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller kriterier för hur den ska utses föreskrivas i unionsrätten eller nationell rätt. Direktivet ger alltså möjlighet att fastställa personuppgiftsansvaret i författning.⁸⁵

Ändamålsbestämmelser

Utredningen om 2016 års dataskyddsdirektiv har gjort överväganden som lett fram till att man inom direktivets område och för de registerförfattningar som omfattats av utredningens uppdrag har föreslagit ändringar i bestämmelser som för närvarande, och enligt sin ordalydelse, betraktas som s.k. ändamålsbestämmelser. Vi anser att utredningens resonemang om ändamålsbestämmelser, som föregåtts av Informationshanteringsutredningens överväganden, är rimliga i och för sig. Utredningen om 2016 års dataskyddsdirektiv har dock inte gjort bedömningen att primära ändamålsbestämmelser, med det innehåll de har i dag, skulle strida mot direktivet. Oavsett om man uppfattar dessa bestämmelser som ändamålsbestämmelser eller preciseringar av personuppgiftsbehandlingens rättsliga grunder (som utredningen menar att man bör göra) fyller de, som utredningen påpekar, en viktig funktion som avgränsande ramar för behandlingen. Sådana ramar innebär bl.a. ett skydd för den personliga integriteten och kan därmed inte anses strida emot direktivets krav.⁸⁶ Utredningen menar dock att

⁸⁴ Jfr exempelvis Utredningen om 2016 års dataskyddsdirektivs överväganden och förslag till ändringar i lagen (2014:400) om Polismyndighetens elimineringsdatabas och lagen (2017:496) om internationellt polisiärt samarbete, SOU 2017:74 s. 133, 184, 753 f. och 755 f.

⁸⁵ Jfr SOU 2017:29 s. 298.

⁸⁶ SOU 2017:29 s. 242 och 253 samt SOU 2017:74 s. 383–392.

sekundära ändamålsbestämmelser som avser vidarebehandling inom det nya dataskyddsdirektivets tillämpningsområde inte är förenliga med direktivet eftersom artikel 4.2 kräver en proportionalitetsbedömning. Däremot anser utredningen att sekundära ändamålsbestämmelser som avser utlämnanden som i stället omfattas av dataskyddsförordningen kan behållas i och för sig.⁸⁷ Eftersom några sekundära ändamålsbestämmelser inom det nya dataskyddsdirektivets område inte förekommer i de författningar som ingår i vårt uppdrag ser vi inte anledning att överväga den frågan.

Ytterligare stöd för att i vart fall primära ändamålsbestämmelser är tillåtna i nationell rätt är direktivets artikel 8.2 som anger att nationell rätt ska specificera ändamålen för behandlingen.⁸⁸

Utlämnande av personuppgifter

Liksom i registerförfattningar inom dataskyddsförordningens tillämpningsområde finns i registerförfattningar inom det nya dataskyddsdirektivets tillämpningsområde bestämmelser som reglerar utlämnande för att möjliggöra informationslämnande som annars skulle omfattas av sekretess. Sådana bestämmelser avser alltså inte att reglera dataskydd i och för sig. Sekretessbrytande bestämmelser innebär inte heller per automatik att det är tillåtet att behandla personuppgifter automatiserat. Samtidigt innebär sekretessbrytande bestämmelser att det finns grundläggande förutsättningar för ett informationsutbyte som innehåller personuppgifter, ett informationsutbyte som annars hade varit förhindrat av sekretess, jfr våra överväganden i avsnitt 2.5.4. Sekretessbrytande reglering i nationell rätt förhindras inte av direktivet. Utredningen om 2016 års dataskyddsdirektiv har överfört eller låtit sådana bestämmelser stå kvar i de registerförfattningar inom det nya dataskyddsdirektivets tillämpningsområde som ingår i deras uppdrag.⁸⁹

Som vi redan berört är en särskild fråga hur man ska se på bestämmelser som reglerar utlämnande av personuppgifter som

⁸⁷ SOU 2017:74 s. 392 respektive s. 397.

⁸⁸ Som Utredningen om 2016 års dataskyddsdirektiv anför kan det i och för sig anses oklart vilka *krav* på preciserade ändamålsbestämmelser i nationell rätt som direktivet ställer (SOU 2017:29 s. 244). Det är dock en annan fråga än den om direktivet *tillåter* ändamålsbestämmelser, preciserade eller inte.

⁸⁹ SOU 2017:74 s. 324 f.

först behandlats för ändamål inom det nya dataskyddsdirektivets tillämpningsområde och sedan utlämnas för syften som faller utanför direktivet. Detta tas upp i direktivets artikel 9. Utredningen om 2016 års dataskyddsdirektiv har anfört att artikel 9 innebär att prövningen av om behandlingen är tillåten ska göras endast med utgångspunkt i förordningen och att behandlingen därmed ska ses som en ursprungsbehandling. Utredningen konstaterar att det inte kan råda någon tvekan om att det är möjligt att i registerförfattningar reglera utlämnandefrågor som avser att uppgifter som från början behandlats inom det nya dataskyddsdirektivets tillämpningsområde senare lämnas ut för syften som inte omfattas av direktivet.⁹⁰ Vi delar denna bedömning. I artikel 9 anges att behandling för syften utanför direktivets tillämpningsområde inte får ske om den inte är tillåten enligt nationell rätt eller av unionsrätten.

Utredningen om 2016 års dataskyddsdirektiv föreslår en generell reglering av behandling för syften inom dataskyddsförordningens tillämpningsområde som innebär att sådan behandling får ske om det är säkerställt att behandlingen är nödvändig och proportionerlig för det ändamålet (2 kap. 22 § brottsdatalogen). En sådan bedömning av nödvändighet och proportionalitet behöver dock inte göras om en skyldighet att lämna uppgifter följer av lag eller förordning. (2 kap. 22 § tredje stycket).⁹¹

Vilka uppgifter som får behandlas

Registerförfattningar på direktivets område kan, liksom på förordningens, vara vad som kan kallas informationshanteringsförfattningar. Sådana tar sällan upp någon specificering av vilka personuppgifter som får behandlas (med undantag för särreglering av känsliga personuppgifter). I renodlade registerförfattningar brukar det däremot anges mer exakt vilka uppgifter som ska tas upp i ett visst register. Att sådana specificeringar är tillåtna får

⁹⁰ SOU 2017:29 s. 295.

⁹¹ SOU 2017:74 s. 190 f. och 393.

anses framgå av artikel 8.2, som anger att nationell rätt ska innehålla preciseringar av vilka personuppgifter som får behandlas.⁹²

Elektroniskt utlämnande av personuppgifter

Det kan i registerförfattningar inom det nya dataskyddsdirektivets tillämpningsområde förekomma reglering av i vilka former utlämnande får ske. Det gäller då vanligen olika former av elektroniskt utlämnande. Som redan redogjorts för (avsnitt 2.5.4) avser *direktåtkomst* en form av utlämnande som bör skiljas från andra former av elektroniskt utlämnande, eftersom direktåtkomst har särskilda rättsliga följder som andra former av elektroniska utlämnanden inte har. Utredningen om 2016 års dataskyddsdirektiv föreslår bestämmelser om elektroniskt utlämnande i skilda registerförfattningar. Sådan särreglering får alltså anses vara förenlig med det nya dataskyddsdirektivet.

Åtkomst inom en myndighet

Bestämmelser som på olika sätt reglerar åtkomsten till personuppgifter inom en myndighet bör, även med utgångspunkt i direktivet, kunna betraktas på samma sätt som sådan reglering i förhållande till dataskyddsförordningen. Det handlar alltså i vart fall om en precisering av artikel 4.1 c (personuppgifter ska vara adekvata, relevanta och inte för omfattande i förhållande till de syften för vilka de behandlas). Man kan också betrakta sådana bestämmelser som en precisering av principen i artikel 4.1 f (personuppgifter ska behandlas på ett sätt som säkerställer en lämplig säkerhet för dem). Utredningen om 2016 års dataskyddsdirektiv föreslår en generell reglering av åtkomst i 3 kap. 6 § brottsdatalagen.

⁹² Vilka mer exakta krav som artikel 8.2 ställer i detta avseende kan alltså ifrågasättas i och för sig, men av bestämmelsen måste i vart fall anses följa att exakta angivelser i författning av att vissa personuppgifter ska behandlas i ett visst sammanhang är förenligt med direktivet.

Bevarande och gallring

I vissa av de författningar som ingår i vårt uppdrag finns gallringsbestämmelser som tar upp en exakt tidpunkt när uppgifter ska gallras. Sådana bestämmelser är förenliga med direktivet, som innehåller både den allmänna principen att personuppgifter inte ska bevaras längre än vad som behövs för det ändamål de behandlas för (artikel 4.1 e) och en skyldighet för medlemsstaterna att fastställa lämpliga tidsgränser för radering av personuppgifter (artikel 5). Av den sistnämnda artikeln följer att om inte tidsgränser föreskrivs ska periodiska översyner av behovet av lagring göras. Artikeln har genomförts i 2 kap. 17 och 18 §§ brottsdatalagen.

Utredningen om 2016 års dataskyddsdirektiv har föreslagit en viss förändring i gallringsbestämmelser i de registerförfattningar som omfattas av utredningens uppdrag. Utredningen anser att begreppet *gallring* i huvudsak inte bör användas i bestämmelser som avser dataskydd. Vi överväger frågor om användandet av ordet *gallring* i avsnitt 5.5 och 6.5.

Bestämmelser som genomför vissa tidigare EU-rättsakter - artikel 60

Det nya dataskyddsdirektivet innehåller en artikel som avser förhållandet till tidigare EU-rättsakter inom området för polisiärt och straffrättsligt samarbete som trätt i kraft före den 6 maj 2016. I artikeln anges att det nya dataskyddsdirektivet inte ska påverka ”särskilda bestämmelser om skydd för personuppgifter” i sådana unionsrättsakter. Man kan fråga sig om formuleringen innebär att vissa andra bestämmelser i sådana rättsakter, om de inte innebär ett ”skydd”, därmed skulle kunna åsidosättas som en följd av det nya direktivet. Exempelvis kan det diskuteras om en EU-rättsakt vars bestämmelser innebär ett utvidgat informationsutbyte inom EU innebär ett skydd för personuppgifter.

Vi gör bedömningen att frågan får liten praktisk betydelse, eftersom flertalet bestämmelser i tidigare EU-rättsakter, som ger en rättslig grund för personuppgiftsbehandling och preciserar den på olika sätt, under alla förhållanden är förenliga med det nya dataskyddsdirektivet. Att tidigare upprättat informationsutbyte ska kunna fortgå och inte förhindras av den nya dataskyddsregleringen torde också vara syftet bakom artikel 60.

2.6.4 Känsliga personuppgifter

Direktivets artikel 10, som avser känsliga personuppgifter, innehåller en liknande reglering som den i artikel 9.1 och 9.2 g i dataskyddsförordningen. Det ställs alltså krav på att sådan behandling ska regleras i nationell rätt och att det ska finnas skyddsåtgärder för den registrerade. Utredningen om 2016 års dataskyddsdirektiv har också föreslagit ett genomförande som i huvudsak överensstämmer med regleringen i den föreslagna dataskyddslagen (jfr 2 kap. 11, 13 och 2 §§ brottsdatalagen med 3 kap. 3 § dataskyddslagen).

Båda EU-rättsakterna kan anses ge ett ganska stort utrymme för medlemsstaterna att utforma bestämmelser avseende känsliga personuppgifter. De generella bestämmelser som föreslås av Utredningen om 2016 års dataskyddsdirektiv torde vara förenliga även med dataskyddsförordningen och på samma sätt torde de föreslagna bestämmelserna i dataskyddslagen kunna användas även i registerförfattningar inom direktivets tillämpningsområde. För myndigheter som kommer att hantera personuppgifter både inom direktivets och förordningens tillämpningsområde och som kommer ha flera olika registerförfattningar att förhålla sig till torde det dock vara en fördel om regleringen är likalydande om det är möjligt. Vi återkommer till denna fråga i avsnitt 3.5.4 och 4.1.5.

2.6.5 Bestämmelser som inte kan behållas

För författningar som reglerar personuppgiftsbehandling inom det nya dataskyddsdirektivets område måste, liksom på dataskyddsförordningens område, hänvisningar till personuppgiftslagen tas bort eftersom den lagen upphävs.⁹³

Hänvisningar till lagen (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen måste också tas bort. Den nämnda lagen innehåller bestämmelser för att genomföra det s.k. dataskyddsrambeslutet, som upphör att gälla i och med att det nya dataskyddsdirektivet ska vara genomfört i nationell rätt (artikel 59 i

⁹³ SOU 2017:39 s. 49 (förslaget till dataskyddslag, ikraftträdande och övergångsbestämmelser p 2) och s. 78.

det nya dataskyddsdirektivet). Utredningen om 2016 års dataskyddsdirektiv har föreslagit att 2013 års lag upphävs.⁹⁴

2.6.6 Den enskildes rättigheter

Det finns likheter mellan det nya dataskyddsdirektivets reglering av den enskildes rättigheter och dataskyddsförordningens. Det nya direktivet innehåller dock ingen sådan rätt att invända mot behandlingen som den som finns i dataskyddsförordningen. Följaktligen kan den enskilde inte heller åstadkomma att behandlingen begränsas i avvaktan på en utredning av om invändningarna är befogade. Det finns heller inga möjligheter att genom nationell rätt inskränka vad direktivet föreskriver om rättelse, radering och begränsning av behandlingen i artikel 16.1–16.3. Vi har därmed ingen anledning att göra några överväganden avseende direktivets reglering på detta område. Brottsdatalagens reglering kommer att genomföra direktivets krav i dessa avseenden.

När det gäller den enskildes rätt till information har direktivet genomförts i brottsdatalagen. Enligt brottsdatalagen gäller undantag från informationsplikten i den utsträckning det är föreskrivet i lag eller författning eller annars framgår av beslut som har meddelats med stöd av författning och om uppgifterna i sådana fall inte får lämnas ut med hänsyn till vissa särskilt uppräknade intressen, bl.a. att förebygga brott. Inom ramen för vårt uppdrag är frågan om informationsskyldighetens omfattning endast aktuell då det gäller lagen om belastningsregister. Våra överväganden finns i avsnitt 5.5.

2.6.7 Behovet av nya bestämmelser

Upplysande bestämmelse om förhållandet till brottsdatalagen

Många registerförfattningar inom det nya dataskyddsdirektivets tillämpningsområde innehåller i dag en bestämmelse om förhållandet till personuppgiftslagen. Personuppgiftslagen kommer,

⁹⁴ SOU 2017:29 s. 56 (förslaget till brottsdatalag, ikraftträdande och övergångsbestämmelser p 2) och s. 145.

inom det nya dataskyddsdirektivets tillämpningsområde, att ersättas av brottsdatalagen. Utredningen om 2016 års dataskyddsdirektiv föreslår bestämmelser, i de lagar som omfattas av den utredningens uppdrag, som anger att registerförfattningen i fråga gäller utöver brottsdatalagen.⁹⁵ Vi delar utredningens bedömning att det är lämpligt att införa en sådan bestämmelse i flertalet av de författningar som ingår i vårt uppdrag och som omfattas av direktivets tillämpningsområde, i vart fall när lagstiftningen sedan tidigare innehåller hänvisningar till personuppgiftslagen. I författningar som däremot idag inte alls innehåller hänvisningar till personuppgiftslagen och inte heller i övrigt måste ändras materiellt som en följd av genomförandet av det nya dataskyddsdirektivet, menar vi dock att upplysande bestämmelser kan undvaras. Detta gäller särskilt om författningen i fråga endast till en begränsad del reglerar frågor som har med personuppgiftsbehandlingen i sig att göra.

Tillsyn

Bestämmelser om tillsyn finns i 5 kap. i brottsdatalagen. Tillsynsområdet framgår av definitionen av *tillsynsmyndighet* i 1 kap. 6 §. Av definitionen följer att området för tillsyn är både brottsdatalagen och registerförfattningar inom brottsdatalagens tillämpningsområde.⁹⁶ Det krävs alltså inte några bestämmelser i registerförfattningarna för att tillsyn ska kunna utövas på sätt som följer av det nya dataskyddsdirektivet.

Sanktionsavgifter

Utredningen om 2016 års dataskyddsdirektiv har föreslagit att ett administrativt sanktionssystem – sanktionsavgift – ska införas i brottsdatalagen. Utredningen anför att det nya dataskyddsdirektivet ställer krav på effektiva sanktioner och att möjligheten att begära skadestånd inte uppfyller detta krav, samtidigt som en (ytterligare) kriminalisering inte är lämplig. Utredningen anför också att det ligger nära till hands att överväga samma sanktions-

⁹⁵ SOU 2017:29 s. 141.

⁹⁶ A. a. s. 433 f.

system inom det nya direktivets tillämpningsområde som inom dataskyddsförordningen, där Dataskyddsutredningen föreslår att sanktionsavgifter ska kunna tas ut även av myndigheter.⁹⁷

Bestämmelser om sanktionsavgifter finns i 6 kap. brottsdatalagen. I kapitlets inledande paragraf anges att sanktionsavgift kan tas ut vid överträdelse av vissa bestämmelser i brottsdatalagen. Det gäller exempelvis flertalet av de grundläggande kraven på behandling av personuppgifter i 2 kap. Utöver vad som följer av 6 kap. 1 § brottsdatalagen har Utredningen om 2016 års dataskyddsdirektiv gjort bedömningen att det i vissa fall finns anledning att i registerförfattningar särskilt ange att överträdelser av bestämmelser i dessa författningar kan medföra sanktionsavgift. Det gäller överträdelser av bestämmelserna om tillåtna rättsliga grunder för behandling av personuppgifter och hur länge personuppgifter får behandlas, otillåten behandling av känsliga personuppgifter och otillåtna sökningar.⁹⁸

De registerförfattningar som ingår i vårt uppdrag och som vi föreslår ska gälla utöver brottsdatalagen är författningar som avser behandling i tydligt avgränsade behandlingssystem (belastningsregistret, misstankeregistret och Schengens informationssystem). Vilka personuppgifter som får behandlas och under hur lång tid är väl preciserat, liksom användningen av personuppgifter ur registren. Behovet att införa särskilda sanktionsmöjligheter i registerförfattningarna bör ses mot bakgrund av att personuppgiftsbehandlingen på så sätt får anses vara relativt begränsad.

Vi bedömer vidare att sanktionssystemet i brottsdatalagen kan tillämpas även utan att särskilda hänvisningar görs dit. Om personuppgifter behandlas på ett sätt som strider mot författningarna torde sanktionsavgift kunna komma i fråga exempelvis för att det inte finns någon rättslig grund för behandlingen, för att personuppgifterna behandlats under för lång tid eller för att myndigheten inte vidtagit tekniska eller organisatoriska åtgärder för att se till att behandlingen är författningssänlig. Det finns vidare alltid möjlighet för tillsynsmyndigheten att förelägga den personuppgiftsansvarige att vidta åtgärder. Om sådana förelägganden inte följs kan sanktionsavgifter komma i fråga på den grunden. När det gäller

⁹⁷ SOU 2017:29 s. 492–501.

⁹⁸ SOU 2017:74 s. 349–352.

efterlysta personer (som behandlas med stöd av efterlysningsskugörelsen) kommer uppgifter om dem, om de behandlas i brottsbekämpande verksamhet, att omfattas av polisens brottsdatalags tillämpningsområde och därmed även sanktioneras genom den lagens bestämmelser (se vidare kap. 13).

Vi menar att om sanktionsavgifter ska införas är det tillräckligt, i vart fall i förhållande till de författningar som ingår i vårt uppdrag, att brottsdatalagen innehåller bestämmelser om sanktionsavgifter. Vi föreslår därför inga särskilda sanktionsbestämmelser för registerförfattningar som omfattas av det nya dataskyddsdirektivets tillämpningsområde.

Rättelse, radering, begränsning av behandlingen och skadestånd

Det nya dataskyddsdirektivets bestämmelser om rättelse, radering, begränsning och skadestånd (artiklarna 16 och 56) genomförs i brottsdatalagen. Bestämmelser om rättelse och begränsning av behandlingen av personuppgifter finns i 4 kap. 9 § brottsdatalagen. Eftersom bestämmelsen är generellt avfattad och inte begränsad till behandling som sker enbart enligt brottsdatalagen, behövs det ingen hänvisning till bestämmelsen i registerförfattningarna för att den ska kunna tillämpas, även om den personuppgift som den registrerade anser vara felaktig eller ofullständig behandlas med stöd av en registerförfattning. När det gäller radering anges däremot i 4 kap. 10 § att personuppgifter ska raderas om de behandlas i strid med vissa uppräknade bestämmelser i 2 kap. Bestämmelsen torde dock kunna tillämpas även vid vissa överträdelser av registerförfattningar. Vidare anges att uppgifter ska raderas om det krävs för att den personuppgiftsansvarige ska utföra en rättslig förpliktelse. Av författningskommentaren till bestämmelsen framgår att en rättslig förpliktelse kan avse en skyldighet som rör hur personuppgifter får behandlas enligt brottsdatalagen, myndighetens registerförfattning eller någon annan författning om ett enskilt register, exempelvis lagen (1998:621) om misstankeregister.⁹⁹ Det behövs alltså inga hänvisningar till bestämmelsen för att den ska bli tillämplig även på personuppgiftsbehandling som sker med stöd av särreglering inom det nya dataskyddsdirektivets tillämpningsområde.

⁹⁹ SOU 2017:29 s. 727.

När det däremot gäller skadestånd gäller brottsdatalagens bestämmelse om skada uppstått vid behandling av personuppgifter i strid med brottsdatalagen. På samma sätt som det i dag hänvisas till personuppgiftslagens bestämmelse om skadestånd i registerförfattningar, måste en motsvarande hänvisning göras i registerförfattningar till 7 kap. 1 § brottsdatalagen. Utredningen om 2016 års dataskyddsdirektiv föreslår genomgående sådana hänvisningar i de registerförfattningar som omfattas av utredningens uppdrag.¹⁰⁰

Överklagande

I 7 kap. 2 § brottsdatalagen föreskrivs att beslut i fråga om rättelse eller komplettering, radering eller begränsning av behandlingen av personuppgifter, som har meddelats av en myndighet i egenskap av personuppgiftsansvarig, får överklagas till allmän förvaltningsdomstol. Detsamma gäller beslut att inte lämna information på begäran av en registrerad, att ta ut avgift för att lämna information eller att inte medge omprövning av ett automatiserat beslut. I 7 kap. 3 § finns en särskild bestämmelse om dröjsmålstanan. Även beslut med stöd av den paragrafen får överklagas. Enligt 7 kap. 4 § brottsdatalagen får tillsynsmyndighetens beslut enligt lagen eller enligt föreskrifter som har meddelats i anslutning till den överklagas till allmän förvaltningsdomstol. I 7 kap. 5 § brottsdatalagen föreskrivs att andra beslut enligt lagen än de nämnda inte får överklagas.

På samma sätt som den enskilde kan begära rättelse, komplettering, radering eller begränsning av behandlingen med stöd av brottsdatalagen, även om behandlingen sker i ett särskilt reglerat register eller enligt en annan registerförfattning, har den enskilde möjlighet att överklaga sådana beslut enligt brottsdatalagen. Det behövs inga hänvisningar i registerförfattningarna för att åstadkomma detta. Vi menar att upplysande hänvisningar om att överklagande regleras i brottsdatalagen är överflödiga i de registerförfattningar som omfattas av vårt uppdrag.¹⁰¹

¹⁰⁰ SOU 2017:74 s. 352 f.

¹⁰¹ Jfr SOU 2017:74 s. 353 f. där utredningen anger skäl till att upplysande bestämmelser om överklagande bör tas in i registerförfattningarna. En upplysande bestämmelse om överklagande föreslås dock inte i exempelvis lagen (2014:400) om Polismyndighetens elimineringsdatabas, se s. 133–136.

3 Kustbevakningsdatalagen och -förordningen

3.1 Vårt uppdrag

Kustbevakningsdatalagen (2012:145) innehåller i dag bestämmelser som rör både Kustbevakningens brottsbekämpande verksamhet och övriga operativa verksamhet (framgår bl.a. av 1 kap. 5 §). Vårt uppdrag gäller de delar av kustbevakningsdatalagen som omfattas av dataskyddsförordningens tillämpningsområde. Personuppgiftsbehandlingen i den brottsbekämpande verksamheten m.m. övervägs av Utredningen om 2016 års dataskyddsdirektiv. Vårt samråd med den utredningen redovisas i avsnitt 3.3.

3.2 Om författningarna

Kustbevakningens uppdrag och befogenheter

Kustbevakningens uppgifter framgår i huvudsak av myndighetens instruktion (förordning [2007:853] med instruktion för Kustbevakningen). Kustbevakningens rättsliga befogenheter, särskilt när det gäller brottsbekämpning, ordningshållning och kontroll och tillsyn, regleras samtidigt i ett flertal andra författningar. Detta beror bl.a. på att Kustbevakningen är den myndighet som getts ett övergripande ansvar för myndighetsutövning till sjöss i det svenska territoriet. En utförlig beskrivning av Kustbevakningens verksamhet och den rättsliga regleringen finns i betänkandet *Kustbevakningens rättsliga befogenheter* (SOU 2008:55). En mycket kort och förenklad beskrivning är att verksamheten är indelad i två huvudområden, sjöövervakning och räddningstjänst. I uppgiften att bedriva sjöövervakning ingår att bistå andra myndigheter med

övervakning, brottsbekämpande verksamhet, ordningshållning samt kontroll och tillsyn enligt vad som närmare framgår av instruktionen och av annan relevant lagstiftning. Av instruktionen framgår också att Kustbevakning medverkar i internationellt samarbete för att utveckla gränskontroll, brottsbekämpning till sjöss, annan sjöövervakning och miljöräddningstjänst (15 § i förordningen med instruktion).¹

Kort om författningarnas innehåll

En allmän utgångspunkt för regleringen av Kustbevakningens personuppgiftsbehandling var att den tekniska utvecklingen och användandet av informationsteknik hade medfört behov av en ny författningsreglering som inte onödigtvis skulle förhindra en ändamålsenlig effektivisering av verksamheten och som skulle ge förutsättningar för ett både nationellt och internationellt informationsutbyte. Vidare ansåg regeringen att en utgångspunkt var att regleringen, såvitt avsåg Kustbevakningens brottsbekämpande verksamhet, skulle motsvara vad som gäller för polisens brottsbekämpande verksamhet.²

Lagen är indelad i fem kapitel. De två första innehåller bestämmelser för all personuppgiftsbehandling som omfattas av lagens tillämpningsområde, bl.a. lagens generella syfte, förhållandet till personuppgiftslagen, personuppgiftsansvar och behandling av känsliga personuppgifter. I det tredje och fjärde kapitlet regleras personuppgiftsbehandlingen i den brottsbekämpande verksamheten och i det femte personuppgiftsbehandlingen inom den övriga operativa verksamheten. I förordningen finns kompletterande bestämmelser om bl.a. tillgång till personuppgifter (behörigheter, sökning och utlämnande), bevarande och gallring.

¹ Se vidare prop. 2011/12:45 s. 39–49.

² A. prop. s. 60 f.

3.3 En ny kustbevakningsdatalag inom dataskyddsförordningens tillämpningsområde

Förslag: En ny kustbevakningsdatalag införs. Den nya lagen ska innehålla i huvudsak den reglering som finns i dagens kustbevakningsdatalag och som omfattas av dataskyddsförordningens tillämpningsområde.

Skälen för förslaget: Som redogjorts för ovan är dagens kustbevakningsdatalag i huvudsak uppdelad efter om personuppgiftsbehandlingen sker i den brottsbekämpande verksamheten eller i den övriga operativa verksamheten. Lagen innehåller också allmänna bestämmelser avseende all personuppgiftsbehandling inom lagens tillämpningsområde. Förordningens bestämmelser är på samma sätt ibland allmänt tillämpliga och ibland en komplettering till en bestämmelse i lagen som avser endast brottsbekämpning eller endast den övriga operativa verksamheten.

Under vårt arbete har det vid samråd med Utredningen om 2016 års dataskyddsdirektiv framkommit att den utredningen ser det som mest ändamålsenligt att dela upp den nuvarande kustbevakningsdatalagen på två författningar. Vi delar den bedömningen. På det sättet kommer bestämmelser som omfattas av det nya dataskyddsdirektivets tillämpningsområde och bestämmelser som kompletterar dataskyddsförordningen att finnas i varsin lag. Som Utredningen om 2016 års dataskyddsdirektiv framfört innebär EU:s dataskyddsreform att uppdelningen av regleringen av Kustbevakningens personuppgiftsbehandling måste göras på ett annat sätt än i dag. Utredningen framhåller att en reglering i två separata lagar blir tydligare och lättare att tillämpa. Utredningen om 2016 års dataskyddsdirektiv har i sitt slutbetänkande lagt fram förslag till ändringar i den nuvarande kustbevakningsdatalagen som innebär att den författningen byter namn till Kustbevakningens brottsdatalag. Kustbevakningens brottsdatalag kommer att omfatta personuppgiftsbehandling som Kustbevakningen i egenskap av

behörig myndighet utför i syfte att bekämpa eller lagföra brott eller upprätthålla allmän ordning och säkerhet.³

Vi lägger alltså fram ett förslag till en ny kustbevakningsdatalag som innehåller bestämmelser som avser personuppgiftsbehandling som inte rör brottsbekämpning, lagföring och upprätthållande av allmän ordning och säkerhet. Vi återkommer till gränsdragningen mellan Kustbevakningens brottsdatalag och vårt förslag till kustbevakningsdatalag i det följande, avsnitt 3.5.

Vi har, som vi tidigare anfört (se avsnitt 2.4) inte sett det som vår uppgift att på nytt pröva frågor om i vilken utsträckning som personuppgiftsbehandlingen överhuvudtaget behöver regleras eller vilket principiellt innehåll som enskilda bestämmelser bör ha. Vår utgångspunkt har varit att bevara så mycket som möjligt av rådande bestämmelser. Kustbevakningen har heller inte, vid vårt samråd med myndigheten, framfört att dagens reglering har några brister som medför praktiska problem i myndighetens verksamhet. Det som framförts från myndighetens sida är att regleringen bör anpassas så mycket som möjligt till vad som gäller för i första hand Polismyndigheten, i andra hand andra myndigheter med brottsbekämpande uppdrag. Som vi närmare redogör för i det följande har vi därför i viss utsträckning föreslagit bestämmelser för den övriga operativa verksamheten som är likalydande med vad som föreskrivs för den brottsbekämpande verksamheten i den föreslagna brottsdatalagen.

3.4 Överväganden om befintliga bestämmelser

Bedömning: Personuppgiftsbehandling i enlighet med kustbevakningsdatalagen, som omfattas av dataskyddsförordningens tillämpningsområde, uppfyller kraven på rättslig grund i förordningens artikel 6.1 och 6.3.

Bestämmelserna i 1 kap. 1, 3–5 §§, 2 kap. 3, 4 och 6–10 §§ och i stort sett hela 5 kap. kustbevakningsdatalagen behöver inte ändras som en följd av dataskyddsförordningens reglering.

³ Utredningens författningsförslag avseende den nuvarande kustbevakningsdatalagen finns i SOU 2017:74 s. 121–132, de grundläggande övervägandena om tillämpningsområdet på s. 473–475.

Undantaget i 5 kap. är hänvisningen till finalitetsprincipen i 5 kap. 2 § tredje stycket som behöver anpassas till att dataskyddsförordningen innehåller en direkt tillämplig reglering av denna princip.

Bestämmelsen i 1 kap. 2 § om tillämpningsområde är i princip förenlig med dataskyddsförordningen i de delar den berör förordningens tillämpningsområde. Bestämmelserna i 2 kap. 1–2 §§ som reglerar förhållandet till personuppgiftslagen är inte längre aktuella när den lagen upphävs. Skyldigheten att utse personuppgiftsombud (2 kap. 5 §) måste utgå som en följd av att dataskyddsförordningen innehåller en motsvarande reglering.

Övriga bestämmelser i den nuvarande kustbevakningsdatalagen (3 och 4 kap.) avser sådan personuppgiftsbehandling som omfattas av det nya dataskyddsdirektivets tillämpningsområde.

Kustbevakningsdataförordningens bestämmelser som berörs av dataskyddsförordningen är förenliga med denna, med undantag för 2 §. Förordningens 8 § innehåller en hänvisning till personuppgiftslagen och måste därför ändras redan av det skälet.

Skälen för bedömningen:

Dataskyddsförordningens krav på rättslig grund

Som vi tidigare anfört (se avsnitt 2.5.2) har Dataskyddsutredningen anfört att det med hänsyn till svensk förvaltningstradition är rimligt att anta att alla uppgifter som utförs av statliga myndigheter i syfte att uppfylla ett uttryckligt uppdrag av riksdag eller regering är av allmänt intresse i dataskyddsförordningens mening. Kustbevakningens uppdrag i olika avseenden framgår av olika författningar, bl.a. myndighetens instruktion. Kustbevakningen utför alltså uppgifter av allmänt intresse i enlighet med dataskyddsförordningens artikel 6.1 e. Kustbevakningens personuppgiftsbehandling får anses nödvändig för att myndigheten ska kunna utföra sina uppgifter och den kan också i förekommande fall vara ett led i myndighetsutövning. Att myndighetens uppdrag och befogenheter är författningsreglerade innebär att dataskydds-

förordningens samtliga krav på behandlingens rättsliga grund (artikel 6.1 och 6.3) är uppfyllda.⁴ Även kustbevakningsdatalagen bör anses utgöra en rättslig grund för personuppgiftsbehandlingen. Utöver de författningar som specifikt reglerar Kustbevakningens verksamhet finns också rättsliga grunder i sådan reglering som gäller allmänt för myndigheter, exempelvis skyldigheten att registrera och bevara allmänna handlingar. Vi återkommer till detta angående bestämmelsen i 2 kap. 6 § kustbevakningsdatalagen.

I det följande analyseras om de bestämmelser i kustbevakningsdatalagen som avser den operativa verksamheten, alltså den som inte omfattas av det nya dataskyddsdirektivets tillämpningsområde, är förenliga med dataskyddsförordningen. Som vi tidigare anfört är olika preciseringar av de mer övergripande principer som finns i förordningen tillåtna enligt artikel 6.2. Däremot är bestämmelser som endast upprepar något som redan framgår av förordningen inte längre möjliga att ha kvar i nationell rätt, eftersom detta strider mot principen om att förordningar är direkt tillämpliga och inte får implementeras i nationell rätt (se vidare avsnitt 2.3.2). Undantaget är om delar av förordningens bestämmelser kan införas med stöd av de uttalanden som finns i förordningens skäl 8.

Kustbevakningsdatalagen innehåller också några bestämmelser som inte omfattas av vare sig dataskyddsförordningens eller det nya dataskyddsdirektivets tillämpningsområde, exempelvis reglering av föreskriftsrätt. Även sådana bestämmelser tas upp i redogörelsen nedan.

Lagens syfte, tillämpningsområde m.m. (1 kap.)

Lagens första paragraf beskriver det allmänna syftet med regleringen. Som anförts i avsnitt 2.5.4 kan sådana övergripande bestämmelser om syfte, som återfinns i många registerförfattningar, inte anses strida mot dataskyddsförordningen. Att lagens

⁴ Som tidigare beskrivits regleras Kustbevakningens verksamhet och befogenheter i flera författningar, däribland myndighetens instruktion. Samtliga författningar som möjliggör att Kustbevakningen vidtar åtgärder i någon bemärkelse kan anses vara rättsliga grunder för verksamheten och därmed för personuppgiftsbehandlingen i enlighet med artikel 6.3.

tillämpningsområde anges i 2 § är förenligt med dataskyddsförordningen, se vidare avsnitt 2.5.4.

I 2 § tredje stycket anges att kustbevakningsdatalagens bestämmelser är subsidiära till bestämmelser i lagen (2017:496) om internationellt polisiärt samarbete eller föreskrifter till den lagen. Som framgår av andra avsnitt i denna promemoria (exempelvis avsnitt 7.2) är det inte självklart att begreppet *polisiärt samarbete* omfattar enbart samarbete för brottsbekämpning eller andra syften som omfattas av det nya dataskyddsdirektivets tillämpningsområde. Bestämmelser om uppgiftsutbyte i lagen om internationellt polisiärt samarbete (6 kap.–10 kap.) rör dock enbart uppgiftsutbyte för brottsbekämpande ändamål. Lagen om internationellt polisiärt samarbete har alltså endast relevans i förhållande till personuppgiftsbehandlingen i den brottsbekämpande verksamheten, som kommer att regleras i Kustbevakningens brottsdatalag.

Bestämmelsen i 2 a § rör tillämpningen av lag (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polis-samarbete och straffrättsligt samarbete inom Europeiska unionen. Denna lag kommer att upphävas i samband med att det nya dataskyddsdirektivet genomförs och bestämmelsen blir alltså inaktuell i framtiden.⁵

Av 3 § följer att vissa av lagens bestämmelser gäller även för juridiska personer. Eftersom behandling av uppgifter rörande juridiska personer inte omfattas av dataskyddsförordningens tillämpningsområde berörs inte heller denna bestämmelse av förordningens reglering i och för sig. Den kan därmed behållas i nationell rätt, se vidare våra allmänna överväganden, avsnitt 2.5.4.

I 4 § finns en definition av uttrycket *gemensamt tillgängliga uppgifter*. För sådana uppgifter gäller sedan särskilda dataskyddsbestämmelser. Att en nationell lagstiftning innehåller ett särskilt skydd för uppgifter som flera personer inom en myndighet har tillgång till får anses vara en sådan precisering av behandlingen som är tillåten i enlighet med artikel 6.2 (se vidare avsnitt 2.5.4).

Bestämmelsen i 5 § innehåller en beskrivning av lagens disposition. Som vi återkommer till i avsnitt 3.5.1 blir bestämmelsen inaktuell när regleringen av kustbevakningens personuppgiftsbehandling delas upp på två författningar.

⁵ Se vidare våra allmänna överväganden samt SOU 2017:29 s. 145.

Förhållandet till personuppgiftslagen (2 kap. 1 och 2 §§)

Som vi tidigare konstaterat måste alla hänvisningar till personuppgiftslagen utgå när denna lag upphör att gälla. Istället bör ny författningsreglering införas som klargör förhållandet till bl.a. dataskyddsförordningen. Våra förslag till författningsreglering finns i avsnitt 3.5.2.

Tillgång till personuppgifter och personuppgiftsansvar (2 kap. 3 och 4 §§)

I 3 § finns en allmän bestämmelse om tillgången till personuppgifter, som ska begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter. En sådan bestämmelse får anses vara en sådan precisering av principen om integritet och konfidentialitet (artikel 5.1 f) som är tillåten enligt 6.2 dataskyddsförordningen. Att regeringen eller den myndighet regeringen bestämmer kan meddela föreskrifter berörs inte av dataskyddsförordningen, eftersom förordningen inte reglerar frågor om normhierarki (se även avsnitt 2.5.4).

Att Kustbevakningen pekats ut som personuppgiftsansvarig (4 §) är förenligt med dataskyddsförordningen (se vidare avsnitt 2.5.4).

Skyldigheten att utse personuppgiftsombud (2 kap. 5 §)

Begreppet *personuppgiftsombud* kommer i och med de nya EUrättsakterna att ersättas med *dataskyddsombud*. Skyldigheten att utse ett sådant ombud kommer att framgå av artikel 37.1 a i dataskyddsförordningen. Bestämmelsen i 2 kap. 5 § måste alltså utgå (se även avsnitt 2.5.7).

Behandling för diarieföring (2 kap. 6 §)

Enligt 2 kap. 6 § får personuppgifter alltid behandlas för diarieföring och om uppgifterna har lämnats i en anmälan eller liknande och behandlingen är nödvändig för handläggningen. Bakgrunden till bestämmelsen är den generella skyldighet alla myndigheter har att dels diarieföra allmänna handlingar, dels kommunicera med

enskilda som kontaktar myndigheten. Sådan behandling av personuppgifter kan inte alltid hänföras till vad som behövs eller är nödvändigt för ändamål som rör myndighetens egentliga verksamhet. Därför ansåg regeringen att det fanns ett behov, som det får förstås främst för tydlighets skull, av en bestämmelse som klargjorde detta förhållande även i kustbevakningsdatalagen.⁶ Att i lagstiftning föreskriva ändamål för behandlingen måste, som anförs i avsnitt 2.5.4, anses vara förenligt med dataskyddsförordningen.

Behandling av känsliga personuppgifter (2 kap. 7 § och 5 kap. 4 §)

I våra allmänna överväganden (avsnitt 2.5.6) har vi beskrivit dataskyddsförordningens reglering av vad som däri kallas *särskilda kategorier av personuppgifter* och den reglering som Dataskyddsutredningen föreslår avseende denna särskilda kategori, som i svensk rätt kommer att benämnas *känsliga personuppgifter*. Vi menar att de bestämmelser som rör känsliga personuppgifter i dagens kustbevakningsdatalag i sak är jämförbara med vad som föreslås av Dataskyddsutredningen. Det skulle alltså vara möjligt i och för sig att behålla dessa bestämmelser oförändrade (2 kap. 7 § och 5 kap. 4 §). Det finns samtidigt andra alternativ, som vi överväger i kommande avsnitt.

I 2 kap. 7 § finns också en bestämmelse om att uppgifter som beskriver en persons utseende ska utformas på ett objektivt sätt med respekt för människovärdet. Bestämmelsen rör inte personuppgiftsbehandlingen i sig och behöver därmed inte ändras som en följd av att dataskyddsförordningen ska börja tillämpas.

Elektroniskt utlämnande och särskiljande av uppgifter som rör brottsbekämpning (2 kap. 8–10 §§)

Bestämmelserna i 2 kap. 8 och 9 §§ rör utlämnande på medium för automatiserad behandling, bl.a. direktåtkomst. Bestämmelserna får anses vara sådana preciseringar av behandlingen som är förenliga med dataskyddsförordningens artikel 6.2 (se vidare avsnitt 2.5.4.). Detsamma gäller 2 kap. 10 §, som anger att personuppgifter ska

⁶ Prop. 2011/12:45 s. 92.

behandlas på ett sådant sätt att det klart framgår om behandlingen rör brottsbekämpning eller annan operativ verksamhet. Denna bestämmelse kan sägas vara en precisering av artikel 5.1 b – det ska vid insamling och vidarebehandling av personuppgifter stå klart för vilka ändamål behandlingen sker.

Bestämmelserna är alltså i och för sig förenliga med dataskyddsförordningen. Vi lämnar dock förslag på vissa förändringar avseende elektroniskt utlämnande samt överväger om 2 kap. 10 § ska överföras till den nya kustbevakningsdatalagen eller inte i nästa avsnitt.

Ändamål, direktåtkomst och utlämnande (5 kap)

De flesta bestämmelser i 5 kap. är sådana som kan anses vara preciseringar i nationell rätt av principer i dataskyddsförordningen och därmed förenliga med förordningen i enlighet med artikel 6.2 (se vidare avsnitt 2.5.4). Det gäller:

- ändamål för behandlingen (primära och sekundära, 1 och 2 §§)
- direktåtkomst (5 §)
- utlämnande (6 §)
- bevarande och gallring (7 §).

Reglering av primära och sekundära ändamål och utlämnande kan också ses som rättsliga grunder för behandlingen, se vidare avsnitt 2.5.4. Där överväger vi också sekundära ändamålsbestämmelsers förenlighet med artikel 6.4 i dataskyddsförordningen.

I 5 kap. 3 § finns en bestämmelse som snarast får uppfattas som en upplysning av innebörd att om misstanke om brott uppstår vid behandling av personuppgifter i den övriga operativa verksamheten, ska 3 och 4 kap. tillämpas på den fortsatta behandlingen. En sådan upplysande bestämmelse rör inte dataskyddet som sådant och kan därmed i och för sig behållas. Som framgår av våra överväganden i nästa stycke menar vi dock att den inte behövs i en ny kustbevakningsdatalag.

Bestämmelsen om sökning i 5 kap. 4 § har behandlats ovan.

Särskilt om hänvisningen till finalitetsprincipen

I 5 kap. 2 § tredje stycket finns vad som kan kallas en hänvisning till finalitetsprincipen – bestämmelsen anger att utöver de uppräknade sekundära ändamålen får uppgiftsbehandling i ett enskilt fall ske för att tillhandahålla information för något annat ändamål, under förutsättning att ändamålet inte är oförenligt med det ändamål för vilket uppgifterna samlades in.

Denna, och andra liknande bestämmelser i andra registerförfattningar, har tillkommit för att sekundära ändamål inte ska uppfattas som uttömmande. Regeringen har dock gett uttryck för att bestämmelsen i och för sig inte är nödvändig för att uppnå detta syfte, utan att det för myndigheter vars registerförfattningar inte innehåller en liknande hänvisning ändå är möjligt att tillämpa finalitetsprincipen – under förutsättning att personuppgiftslagen i denna del är tillämplig på myndighetens personuppgiftsbehandling.⁷

Frågan är nu för vår del, om den aktuella bestämmelsen i kustbevakningsdatalagen kan behållas oförändrad, om den kan tas bort utan att det avsedda rättsläget förändras eller på vilket sätt den annars kan modifieras för att anpassas till dataskyddsförordningen.

Finalitetsprincipen har utvecklats i dataskyddsförordningen i förhållande till hur principen formuleras i 1995 års dataskyddsdirektiv. I dataskyddsförordningen finns den grundläggande principen i artikel 5.1 b. Nyheten i förhållande till 1995 års direktiv är att det för vidarebehandling som inte har direkt stöd i nationell rätt (eller unionsrätten) finns anvisningar i artikel 6.4 om vad den personuppgiftsansvarige särskilt ska beakta vid bedömningen av det nya ändamålets förenlighet med det ursprungliga ändamålet för behandling.

Som vi tidigare anfört anser vi att det ofta inte är möjligt att i nationell rätt endast återupprepa vad som redan står i en direkt tillämplig förordning. Ett återgivande av förordningens ordalydelse kan dock i vissa fall motiveras med hänvisning till dataskyddsförordningens skäl 8. Där anges att medlemsstaterna kan införliva delar av förordningen i nationell rätt om det behövs för samstämmigheten och för att göra nationella bestämmelser begripliga för tillämparen. Detta gäller, som det får förstås, i de fall medlems-

⁷ Prop. 2002/03:135 s. 56, jfr s. 160.

staterna har möjlighet enligt förordningen att precisera eller begränsa förordningens bestämmelser i nationell rätt. Bestämmelsen i 5 kap. 2 § tredje stycket innebär en viss begränsning av myndighetens möjligheter i förhållande till dataskyddsförordningen eftersom den anger att behandling utanför de särskilt angivna sekundära ändamålen bara ska ske i enskilda fall. Begränsningen som sådan är tillåten enligt förordningen (se vidare avsnitt 2.5.3). Att behålla bestämmelsen oförändrad skulle möjligen kunna motiveras med det som sägs i skäl 8. Vi anser dock inte att det är lämpligt, eftersom bestämmelsen i sin nuvarande utformning skulle kunna ge intryck av att de bedömningsgrunder som anges i artikel 6.4 inte är tillämpliga. Vi gör vidare överväganden i avsnitt 3.5.⁸

Bestämmelser i förordningen

I 1 § anges förordningens syfte m.m. Bestämmelsen avser inte personuppgiftsbehandlingen i sig och påverkas därmed inte av dataskyddsförordningen.

I 3–5 §§ finns bestämmelser om behörigheter för tillgång till personuppgifter och sökning bland personuppgifter som i huvudsak avser att Kustbevakningen får meddela närmare föreskrifter i dessa frågor. Som vi anfört i våra generella övervägden påverkas inte bestämmelser om föreskriftsrätt av dataskyddsförordningen.

Bestämmelserna i 6 och 7 §§ avser tillämpningen av bestämmelser i 4 kap. i lagen, som avser personuppgiftsbehandlingen i den brottsbekämpande verksamheten. Dessa bestämmelser ska alltså inte överföras till en förordning som avser övrig operativ verksamhet.

I 8–11 §§ finns bestämmelser som närmare preciserar förutsättningarna för direktåtkomst och annat elektroniskt utlämnande av personuppgifter. Som vi tidigare anfört får bestämmelser som närmare preciserar i vilken elektronisk form personuppgifter får

⁸ Flera andra utredningar lämnar förslag och/eller gör överväganden avseende motsvarande bestämmelser i andra registerlagar. Inte alla är samstämmiga, utan flera olika modeller presenteras för hur hänvisningen till finalitetsprincipen ska utformas med beaktande av dataskyddsförordningens reglering. Se vidare exempelvis Ds 2017:19 s. 78 och 161 f., Ds 2017:26 s. 21 och 42 och Ds 2017:28 s. 28 och 107 f.

lämnas ut anses vara förenliga med dataskyddsförordningen i enlighet med artikel 6.2.

I 12 och 13 §§ finns allmänna bestämmelser om gallring som avser både brottsbekämpande och övrig operativ verksamhet. Som vi redogjort för i avsnitt 2.5.4 förhindrar inte dataskyddsförordningen att mer preciserade bestämmelser om gallring förekommer i nationell rätt. Det finns heller inget som hindrar mer preciserade bestämmelser om bevarande för arkivering, eller bevarande för historiska, statistiska eller vetenskapliga ändamål. Alla dessa ändamål anses i sig vara förenliga med de ursprungliga ändamålen för behandling, men innebär samtidigt inte någon skyldighet för medlemsstaterna att bevara personuppgifter. Att ha bestämmelser som preciserar när bevarande ska ske för sådana ändamål är alltså förenligt med dataskyddsförordningen.

Bestämmelserna om gallring i 14–18 §§ rör den brottsbekämpande verksamheten och berörs därmed inte av dataskyddsförordningens tillämpningsområde.

Förordningens 19 och 20 §§ avser Kustbevakningens möjligheter att meddela närmare föreskrifter. Bestämmelserna rör alltså inte personuppgiftsbehandlingen i sig och berörs därmed inte av dataskyddsförordningen.

Merparten av bestämmelserna i kustbevakningsdataförordningen som omfattas av dataskyddsförordningens tillämpningsområde är alltså i och för sig förenliga med förordningen. I 8 § finns dock en hänvisning till personuppgiftslagen och bestämmelsen måste ändras redan av den anledningen. Det finns också skäl att göra vissa andra förändringar i den nuvarande förordningens bestämmelser. Vi lämnar förslag i avsnitt 3.5.8.

Förordningens 2 §

I 2 § finns en bestämmelse om samråd med Datainspektionen när kustbevakningen planerar att ta i drift nya it-system av större omfattning eller göra betydande förändringar i befintliga system. I dataskyddsförordningen finns en omfattande reglering av den personuppgiftsansvariges skyldigheter när det gäller säkerhet (artikel 25), konsekvensbedömningar och samråd med tillsynsmyndigheten (artikel 35 och 36). Regleringen i kustbevaknings-

dataförordningen kan enligt vår mening inte uppfattas som en precisering av något som föreskrivs i förordningen, utan får istället betraktas som en sådan likartad reglering som inte längre får förekomma i nationell rätt.

3.5 Överväganden om och förslag till bestämmelser i en ny kustbevakningsdatalag och -förordning

3.5.1 Lagens tillämpningsområde och huvudsakliga innehåll

Förslag: Den nya kustbevakningsdatalagen ska innehålla bestämmelser som i huvudsak överensstämmer med bestämmelserna i 1 kap. 1, 2, 3 och 4 §§, 2 kap. 3, 4, 6–9 §§ och 5 kap. i den nuvarande kustbevakningsdatalagen.

Lagens tillämpningsområde ska i stort överensstämma med tillämpningsområdet för det nuvarande 5 kap. Från lagens tillämpningsområde undantas sådan personuppgiftsbehandling som omfattas av Kustbevakningens brottsdatalag.

Hänvisningar till Kustbevakningens brottsbekämpande verksamhet ska anpassas till utformningen av tillämpningsområdet för Kustbevakningens brottsdatalag.

Bedömning: Utöver våra förslag avseende information till den registrerade föranleder dataskyddsförordningens artiklar om rättigheter för den registrerade inga nya bestämmelser eller författningsändringar i förhållande till den nuvarande kustbevakningsdatalagen.

Skälen för förslaget och bedömningen:

En ny lag – huvudsakligt innehåll och struktur

Som vi konstaterat ovan anser vi att flertalet bestämmelser som finns i den nuvarande kustbevakningsdatalagen och som berör den personuppgiftsbehandling som faller under dataskyddsförordningens tillämpningsområde är förenliga med förordningen. De bör därför fortsätta att gälla och, i enlighet med vad vi anfört i avsnitt

3.3, tas in i en ny lag. Det gäller bestämmelser i 1 kap. 1, 2, 3 och 4 §§, 2 kap. 3–4 och 6–9 §§ och i stort sett hela 5 kap. Bestämmelserna kan alltså tas in i den nya lagen i huvudsak oförändrade. Vi återkommer i avsnitt 3.5.2–3.5.7 med särskilda överväganden och förslag om hur bestämmelser om ändamål, känsliga personuppgifter, elektroniskt utlämnande, information till den registrerade och längsta tid för behandling av personuppgifter ska utformas i den nya lagen.

Utöver vissa förändringar i enskilda bestämmelser, som vi alltså återkommer till i de följande avsnitten, innebär vårt lagsförslag i förhållande till den nuvarande kustbevakningsdatalagen vissa ändringar i den nya lagens struktur. Eftersom antalet bestämmelser blir begränsat, till följd av att personuppgiftsbehandlingen i den brottsbekämpande verksamheten regleras i en egen lag, behöver den nya lagen inte vara kapitelindelas. När kapitelindelningen försvinner är det också befogat att placera vissa bestämmelser i en annan ordningsföljd än tidigare, för att göra författningen mer lättläst. Exempelvis bör sökförbudet för känsliga personuppgifter placeras i anslutning till den grundläggande bestämmelsen om behandling av sådana uppgifter.

Lagens tillämpningsområde och andra hänvisningar till den brottsbekämpande verksamheten

Som tidigare nämnts är dagens kustbevakningsdatalag uppdelad mellan personuppgiftsbehandling i den brottsbekämpande verksamheten och personuppgiftsbehandling i den övriga operativa verksamheten (framgår av 1 kap. 2 och 5 §§ samt lagens kapitelindelning). Denna uppdelning stämmer inte helt och hållet överens med gränsdragningen mellan det nya dataskyddsdirektivets tillämpningsområde och dataskyddsförordningens. Utredningen om 2016 års dataskyddsdirektiv har föreslagit ett tillämpningsområde för brottsdatalagen som till viss del överensstämmer med vad som beskrivs som *brottsbekämpande verksamhet* enligt kustbevakningsdatalagen, nämligen *förebygga, förhindra eller upptäcka brottslig verksamhet och utreda eller beivra brott*. Istället för *beivra brott* används dock uttrycket *lagföra brott* i brottsdatalagen. Brottsdatalagen, och därmed register-

författningar inom brottsdatalagens övergripande tillämpningsområde, ska därtill omfatta, såvitt nu är av intresse,⁹ att *upprätthålla allmän ordning och säkerhet*. Brottsdatalagen avses dock inte omfatta *övervakning* av den allmänna ordningen.

När det gäller den personuppgiftsbehandling som i dag regleras i 5 kap. kustbevakningsdatalagen står det klart att ändamålen i 1 § 2–4 inte faller inom ramen för vare sig brottsbekämpning, lagföring eller upprätthållande av allmän ordning och säkerhet. När det däremot gäller punkten 1 (sjöövervakning m.m.) innefattar den, enligt vad som kan utläsas ur propositionen till lagen, inte bara övervakning utan också upprätthållande av allmän ordning.¹⁰

För att följa den systematik som föreslås av Utredningen om 2016 års dataskyddsdirektiv kan alltså inte nuvarande gränsdragning mellan brottsbekämpning och övrig operativ verksamhet behållas fullt ut. Rent lagtekniskt kan detta åstadkommas genom att lagens tillämpningsområde får omfatta personuppgiftsbehandling i den operativa verksamheten, men inte sådan personuppgiftsbehandling som omfattas av Kustbevakningens brottsdatalag.

Att gränsdragningen mellan de två nya författningarna är något annorlunda avfattad än den mellan dagens 3 och 4 kap. å ena sidan och 5 kap. å den andra för också med sig att första punkten i de sekundära ändamålsbestämmelserna, för närvarande 5 kap. 2 §, får anpassas så att det istället för *brottsbekämpande verksamhet* anges den verksamhet som Kustbevakningens brottsdatalag kommer att omfatta, dvs. brottsbekämpande och lagförande verksamhet samt verksamhet för att upprätthålla allmän ordning och säkerhet.

Gränsdragningen mellan upprätthållande och övervakning av allmän ordning och säkerhet

Som framgår redan av betänkandet *Brottsdatalag* (SOU 2017:29) uppstår en del gränsdragningsfrågor när det gäller att avgöra omfattningen av den nya brottsdatalagens, och tillhörande

⁹ Här bortses från syftet att *verkställa straffrättsliga påföljder*, eftersom Kustbevakningen inte utför några uppgifter inom det området, jfr tillämpningsområdet för Kustbevakningens brottsdatalag (SOU 2017:74 s. 121).

¹⁰ Prop. 2011/12:45 s. 68 och 156 f.

registerförfattningars, tillämpningsområde. Vissa sådana frågor är dock inte nya, utan måste besvaras också vid tillämpningen av dagens regelverk. Exempelvis är kustbevakningsdatalagens 3 och 4 kap., som rör brottsbekämpande verksamhet, inte tillämpliga på kontrollverksamhet, vilket kan förorsaka gränsdragningsproblem, särskilt i den praktiska verksamheten.¹¹ Samma gränsdragningsfrågor kan komma att aktualiseras avseende kustbevakningsdatalagen å ena sidan och Kustbevakningens brottsdatalag å den andra. Vidare har det även tidigare anförts att det kan vara svårt att skilja mellan brottsbekämpande och ordningshållande verksamhet.¹² Med den kommande gränsdragningen tillkommer alltså att inom ramen för ordningshållande verksamhet hålla isär *övervakning* och *upprätthållande* av ordningen. Utredningen om 2016 års dataskyddsdirektiv anför följande.

Utredningen konstaterar i delbetänkandet att det är personuppgiftsbehandling i syfte att upprätthålla allmän ordning och säkerhet som omfattas av brottsdatalagens tillämpningsområde. Utgångspunkten är att det krävs fysisk närvaro på den plats där oordning förekommer eller riskerar att uppstå för att det ska vara fråga om upprätthållande av allmän ordning och säkerhet (se SOU 2017:29 s. 164 f. och 167).

När en kustbevakningstjänsteman ingriper eller är beredd att ingripa vid en konkret ordningsstörning, eller en potentiell sådan störning vid en specifik händelse, är det fråga om upprätthållande av allmän ordning och säkerhet. Personuppgiftsbehandling vid sådan verksamhet bör följaktligen omfattas av tillämpningsområdet för Kustbevakningens brottsdatalag. Detsamma bör gälla vid ingripanden och andra åtgärder för att avvärja konkreta brott.

Den verksamhet som består av allmän övervakning i trygghetskapande syfte och att genom närvaro se till att allmän ordning och säkerhet inte störs, ligger däremot utanför tillämpningsområdet. Sådan övervakning kan utföras t.ex. genom rutinmässig patrullering till sjöss eller flygövervakning eller övervakning med hjälp av kameror eller annan digital utrustning i en ledningscentral. Denna typ av övervakning görs utan att den är inriktad mot en konkret störning eller konkret risk för störning. Allmän övervakning av sådant slag kan emellertid övergå till att ha ett ordningshållande syfte och därmed omfattas av tillämpningsområdet. Så är fallet om ledningscentralen tar radiokontakt med ett övervakat fartyg för att ge anvisningar om t.ex. vilken kurs fartyget ska hålla för att undvika ett avlyst vattenområde. I

¹¹ Prop 2011/12:45 s. 157, jfr SOU 2017:29 s. 198 f.

¹² Se vidare prop. 2009/10:85 s. 75. Det kan noteras att regeringen dock framhöll att gränsdragningsproblemen inte ska överdrivas.

dess fall upprätthålls allmän ordning och säkerhet utan någon fysisk närvaro på platsen där oordning förekommer eller riskerar att uppstå.

Även vid rutinmässig patrullering till sjöss kan det upptäckas ordningsstörningar som kräver ingripande. Det är oftast först vid ingripanden som det blir fråga om att behandla personuppgifter. Gränsdragningen avseende vilket regelverk som gäller i enskilda fall blir ytterst en fråga för tillämpningen.¹³

Behövs särskilda bestämmelser om förhållandet till den brottsbekämpande verksamheten?

Av formuleringen av lagens tillämpningsområde kommer det att framgå att viss del av personuppgiftsbehandlingen i Kustbevakningens operativa verksamhet regleras av en annan lag, Kustbevakningens brottsdatalag. Den nuvarande bestämmelsen i 2 kap. 10 § om att det av behandlingen klart ska framgå om ändamålet är brottsbekämpning bör ses mot bakgrund av att personuppgiftsbehandlingen i hela den operativa verksamheten i dag regleras i samma lag. När det nu blir fråga om två separata författningar menar vi att det inte längre finns något behov av en motsvarande bestämmelse i den nya kustbevakningsdatalagen. Av samma anledning anser vi att bestämmelsen i 5 kap. 3 § inte behövs i den nya lagen. Det framgår redan av de sekundära ändamålsbestämmelserna att personuppgifter får behandlas för att lämnas till den brottsbekämpande verksamheten. Att ett sådant överlämnande behövs om det i den övriga operativa verksamheten uppkommer misstanke om begången brottslighet är självklart.

Den enskildes rättigheter enligt dataskyddsförordningen

Vi har i våra allmänna utgångspunkter (avsnitt 2.5.8) gjort en genomgång av dataskyddsförordningens artiklar som reglerar den enskildes rättigheter, bl.a. till rättelse och begränsning av behandlingen. Som vi angett där har vi inte sett några generella skäl för att inskränka den enskildes rättigheter i något avseende. Inte heller när det gäller Kustbevakningens personuppgiftsbehandling kan vi se att det finns något behov att göra inskränkningar i de rättigheter som

¹³ SOU 2017:74 s. 477 f.

följer av dataskyddsförordningen, utom när det gäller rätten till information, som vi behandlar i det följande (avsnitt 3.5.6).

3.5.2 Förhållandet till dataskyddsförordningen och dataskyddslagen

Förslag: Lagen ska innehålla upplysande bestämmelser som anger att den kompletterar dataskyddsförordningen och att dataskyddslagen gäller vid behandling enligt lagen.

Skälen för förslaget:

En bestämmelse om att lagen kompletterar dataskyddsförordningen

Som vi tidigare anfört anser vi att det i registerförfattningar är lämpligt att ange att den aktuella registerlagen kompletterar dataskyddsförordningen. Den nya kustbevakningsdatalagen bör alltså innehålla en sådan upplysande bestämmelse. Innebörden av att lagen kompletterar dataskyddsförordningen är dels att lagens bestämmelser preciserar dataskyddsförordningens mer allmänna principer för personuppgiftsbehandling, dels att dataskyddsförordningen innehåller reglering av vissa frågor som inte tas upp i kustbevakningsdatalagen, exempelvis avseende rättelse, tillsyn och sanktioner.

Upplysande bestämmelse om dataskyddslagen

I svensk rätt kommer dataskyddsförordningen att, förutom olika registerförfattningar, kompletteras av dataskyddslagen. Dataskyddslagen kommer att innehålla generella bestämmelser om bl.a. sanktioner och tillsyn. Vidare innehåller lagen bestämmelser som i sak överensstämmer med vissa bestämmelser i personuppgiftslagen och som sedan länge gällt även för kustbevakningens personuppgiftsbehandling, exempelvis en bestämmelse om att sekretess innebär att informationslämnande kan underlåtas (5 kap. 1 § dataskyddslagen). Det finns alltså flera bestämmelser i dataskyddslagen

som kan behöva tillämpas för Kustbevakningens personuppgiftsbehandling.

Som vi anfört i våra allmänna överväganden (avsnitt 2.5.9) är vår utgångspunkt att det i registerförfattningar bör hänvisas generellt till dataskyddslagen, trots att vissa bestämmelser i den lagen inte kommer att bli aktuella att tillämpa med avseende på en del myndigheters personuppgiftsbehandling. När det gäller känsliga personuppgifter föreslår vi, som framgår i stycke 3.5.4, en reglering i kustbevakningsdatalagen som i viss mån avviker från dataskyddslagens. Att avvikande bestämmelser i annan författning ska tillämpas istället för dataskyddslagen följer redan av att dataskyddslagen är subsidiär till annan författning.

3.5.3 Primära och sekundära ändamål samt finalitetsprincipen

Förslag: Bestämmelser om primära och sekundära ändamål ska utformas på samma sätt som i dag. Att de sekundära ändamålen inte är uttömmande tydliggörs genom en hänvisning till finalitetsprincipen i dataskyddsförordningen.

Skälen för förslaget:

Ska ändamålsbestämmelser bli rättsliga grunder?

Utredningen om 2016 års dataskyddsdirektiv har föreslagit att de bestämmelser som för närvarande är ändamålsbestämmelser i registerförfattningar under det nya dataskyddsdirektivets tillämpningsområde ska omformuleras så att bestämmelserna i stället avser rättsliga grunder för behandlingen. Vi har övervägt om en motsvarande förändring bör göras även i kustbevakningsdatalagen. Ett skäl för det är att det torde underlätta för tillämparen om de olika regelverken är så likartade som möjligt, jfr våra överväganden om känsliga personuppgifter i nästa stycke. Rent språkligt skulle det inte innebära några stora förändringar i författningstexten – det skulle handla om att ta bort ordet *ändamål* och i stället skriva *rättslig grund* i en rubrik. Vi anser i och för sig att det finns många goda argument för att göra den förändring som föreslås både av

Utredningen om 2016 års dataskyddsdirektiv och av Informationshanteringsutredningen i slutbetänkandet *Myndighetsdatalag* (SOU 2015:39). Samtidigt ingår de föreslagna förändringarna i större och mer övergripande lagstiftningsprodukter – genomförandet av det nya dataskyddsdirektivet i det ena fallet och införandet av en generell myndighetsdatalag i det andra. Förslaget från Utredningen om 2016 års dataskyddsdirektiv bör ses i ljuset av att dataskyddsdirektivet bygger på att de olika ändamålen för behandling av personuppgifter som omfattas av direktivets tillämpningsområde är sinsemellan förenliga. Inom direktivets tillämpningsområde kommer alltså finalitetsprincipen inte att bli tillämplig enligt utredningens uppfattning.¹⁴ Dataskyddsförordningen bygger tvärtom på en uppdelning mellan ursprungliga ändamål och vidarebehandling i enlighet med artikel 6.4. Förordningen använder i dessa och andra sammanhang ordet ändamål, på ett sätt som stämmer väl överens med terminologin i flertalet svenska registerförfattningar. Om ändamålsbestämmelser omvandlas till rättsliga grunder menar vi att det kan uppstå en osäkerhet kring hur vidarebehandling av insamlade uppgifter får ske och hur finalitetsprincipen enligt förordningen ska tillämpas. Inom ramen för vårt begränsade uppdrag anser vi inte att vi har möjlighet att göra den typen av övergripande överväganden som skulle behövas för att genomföra en sådan förändring på förordningens område. Vi föreslår därför ingen ändring av terminologin i kustbevakningsdatalagen, utan menar att dagens reglering av primära och sekundära ändamål bör finnas kvar, i vart fall tills frågan kan övervägas i en annan ordning än inom ramen för vår utredning.

En omformulerad hänvisning till finalitetsprincipen

De primära ändamålen i kustbevakningsdatalagen är uttömmande angivna, men inte de sekundära. Detta markeras genom en hänvisning till att finalitetsprincipen i enskilda fall får tillämpas för att utlämna uppgifter (utlämnande får alltså ske för andra ändamål

¹⁴ SOU 2017:29 s. 248.

än de uppräknade sekundära, om ett annat ändamål inte är oförenligt med insamlingsändamålet).

Som vi redan diskuterat anser vi att hänvisningen till finalitetsprincipen inte kan stå kvar helt oförändrad, utan att någon form av tillägg måste göras för att bestämmelsen inte ska uppfattas som om den utesluter tillämpningen av artikel 6.4. Vi anser inte att det är ett alternativ att låta bestämmelsen helt utgå, eftersom den innehåller en begränsning av finalitetsprincipens tillämpning som inte skulle följa av den direkt tillämpliga förordningen. Syftet med dagens bestämmelse är vidare att tydliggöra att de sekundära ändamålen inte är uttömmande angivna, vilket är ytterligare ett skäl till att bestämmelsen i någon form bör finnas kvar. Vårt förslag är alltså att nuvarande bestämmelse överförs till den nya kustbevakningsdatalagen, men omformuleras så att den i så liten utsträckning som möjligt upprepar vad som framgår av dataskyddsförordningen och i stället hänvisar till artikel 5.1 b och 6.4.

Som tidigare redogjorts för måste varje behandling enligt dataskyddsförordningen vara laglig, vilket för myndigheters del innebär att det ska finnas en rättslig grund för behandlingen som är fastställd i nationell rätt eller i unionsrätten. En vidarebehandling som är förenlig med finalitetsprincipen behöver dock ingen ytterligare rättslig grund och någon bedömning måste alltså inte göras av om behandlingen är laglig enligt artikel 6.1 och 6.3. Detta förhållande framgår av skäl 50.

3.5.4 Känsliga personuppgifter

Förslag: Begreppet känsliga personuppgifter ska omfatta de särskilda kategorier av personuppgifter som särregleras i artikel 9 i dataskyddsförordningen. Känsliga personuppgifter ska få behandlas under i princip samma förutsättningar som i dag men bestämmelsen ska i denna del anpassas till brottsdatalagens reglering. Sökmöjligheterna för sådana personuppgifter ska begränsas på samma sätt som i brottsdatalagen.

Skälen för förslaget: Som vi redogjort för ovan är den nuvarande regleringen av känsliga personuppgifter i kustbevakningsdatalagen i och för sig förenlig med dataskyddsförordningen. De kategorier av

personuppgifter som särregleras i artikel 9 i dataskyddsförordningen överensstämmer dock inte helt med den uppräkningslista som görs i 2 kap. 7 § första stycket kustbevakningsdatalagen. Särregleringen av känsliga personuppgifter bör omfatta samtliga de kategorier av uppgifter som anges i dataskyddsförordningen (se vidare våra allmänna överväganden, avsnitt 2.5.6). Detta bör åstadkommas genom att bestämmelsen i den nya kustbevakningsdatalagen hänvisar till artikel 9.1 dataskyddsförordningen, istället för den nuvarande uppräkningslistan av vilka personuppgifter som avses.

När det gäller förutsättningarna för att få behandla känsliga personuppgifter har Dataskyddsutredningen föreslagit en reglering i 3 kap. 3 § dataskyddslagen som är likartad den som finns i dagens kustbevakningsdatalag. Bestämmelsen som begränsar möjligheten att använda sådana personuppgifter vid sökning i 3 kap. 4 § dataskyddslagen är också likartad vad som gäller enligt 5 kap. 4 § i dagens kustbevakningsdatalag. Förslaget till reglering i brottsdatalagen överensstämmer i huvudsak också med regleringen i nuvarande 2 kap. 7 § kustbevakningsdatalagen och därtill med Dataskyddsutredningens förslag. Det finns alltså åtminstone tre alternativ till en reglering av behandlingen av känsliga personuppgifter i kustbevakningsdatalagen – de bestämmelser som gäller för närvarande, en reglering i enlighet med den i brottsdatalagen eller bestämmelser som motsvarar dataskyddslagens. Det sistnämnda alternativet skulle i praktiken innebära att regleringen av känsliga personuppgifter i kustbevakningsdatalagen kunde tas bort.

För kustbevakningens del anser vi att intresset av en likalydande lagstiftning för brottsbekämpande och annan operativ verksamhet väger tyngst. Förutsättningarna för att behandla känsliga personuppgifter i den operativa verksamheten utanför det brottsbekämpande verksamhetsområdet bör därför utformas i enlighet med brottsdatalagens reglering. Även restriktionerna när det gäller sökning bör utformas på samma sätt som i brottsdatalagen.

3.5.5 Elektroniskt utlämnande av personuppgifter

Förslag: Elektroniskt utlämnande av personuppgifter som inte avser direktåtkomst ska få ske om det inte är olämpligt.

Skälen för förslaget: Som vi redogjort för i avsnitt 2.5.4 är det förenligt med dataskyddsförordningen i och för sig att ha nationella bestämmelser om utlämnande av uppgifter. Det kan vara bestämmelser som preciserar till vilka mottagare utlämnande får ske, i vilka situationer och i vilken form personuppgifter lämnas ut. Bestämmelser om utlämnande i dagens kustbevakningsdatalag är alltså inte oförenliga med dataskyddsförordningen.

När det gäller utlämnande på vad som brukar kallas *medium för automatiserad behandling* föreslår Utredningen om 2016 års dataskyddsdirektiv vissa förändringar i Kustbevakningens brottsdatalag m.fl. registerförfattningar som omfattas av den utredningens uppdrag. I dessa registerförfattningar kommer det för sådant elektroniskt utlämnande att föreskrivas att det får ske *om det inte är olämpligt*, i stället för dagens reglering, som i de flesta fall (liksom i den nuvarande kustbevakningsdatalagen) anger att *enstaka personuppgifter* får lämnas ut på detta sätt. Skälen för utredningens förslag är i korthet att den nuvarande regleringen kritiserats för att vara alltför restriktivt utformad och att detta kan leda till att myndigheterna inte kan dra nytta av effektivitetsvinsterna med ny teknik. Utredningen föreslår också att uttryckssättet i de nuvarande bestämmelserna moderniseras på så sätt att de ska avse *elektroniskt utlämnande* på annat sätt än genom direktåtkomst och inte längre innehålla begreppet *medium för automatiserad behandling*.¹⁵

Den utformning av bestämmelsen om elektroniskt utlämnande som Utredningen om 2016 års dataskyddsdirektiv föreslår är, liksom den nuvarande bestämmelsen, lika förenlig med dataskyddsförordningen som den nuvarande bestämmelsen, eftersom den också utgör en tillåten precisering i enlighet med artikel 6.2 och 6.3. Skälen för att förändra bestämmelsen om utlämnande på medium för automatiserad behandling som Utredningen om 2016

¹⁵ SOU 2017:74 s. 371–375.

års dataskyddsdirektiv lagt fram gör sig lika starkt gällande i den övriga operativa verksamheten som i den brottsbekämpande. Därtill kommer, som vi tidigare framhållit, att det torde underlätta för en myndighet, som har både brottsbekämpande och andra uppdrag, om regleringen av personuppgiftsbehandling är likadant utformad. Vi föreslår därför att bestämmelsen om utlämnande på medium för automatiserad behandling anpassas till regleringen i Kustbevakningens brottsdatalag.

3.5.6 Information till den registrerade

Förslag: Information till den registrerade behöver inte lämnas om insamling av personuppgifter gjorts genom ljud- och bildupptagning, om inte behandlingen i övrigt innebär en direkt identifiering av någon person. Information behöver inte heller lämnas i vissa larmsituationer.

Skälen för förslaget:

Nuvarande inskränkningar av den enskildes rätt till information

I dag gäller personuppgiftslagens bestämmelser om information till den registrerade genom hänvisningen i 2 kap. 2 § 5 kustbevakningsdatalagen. Den registrerades rätt till information är dock inskränkt genom bestämmelsen i 2 § tredje stycket, som anger att information inte behöver lämnas vid behandling som består av insamling genom bild eller ljud och inte heller om uppgifterna samlas in i samband med larm och det med hänsyn till omständigheterna inte finns tid att lämna informationen. När det gäller insamling genom bild och ljud anförde regeringen att Kustbevakningen kan komma att samla in personuppgifter exempelvis genom filmning från kustbevakningsflyget av oljeutsläpp. Regeringen anförde att det i en sådan situation framstår inte bara som orimligt utan också praktiskt ogörligt att informera personer som kan komma att fångas på bild. När det gäller information i samband med larm anförde regeringen bl.a. att information till någon som ringer in för att larma kan försena en behövlig åtgärd och dessutom inte torde intressera personen som larmar. Behovet

av information om personuppgiftsbehandlingen i en larm- eller liknande situation ansågs dock få bedömas från fall till fall.¹⁶

Undantagen från information är välgrundade i och för sig, och företrädare för kustbevakningen har uttryckt att det finns ett stort praktiskt behov att kunna fortsätta tillämpa samma ordning som i dag. Frågan är då om det i och med tillämpningen av dataskyddsförordningen finns möjlighet att göra samma undantag från informationskravet i förordningen som i dag gäller i förhållande till personuppgiftslagen.

Dataskyddsförordningens krav på information

Dataskyddsförordningens krav på information till den registrerade vid insamling av personuppgifter finns i artikel 13 och 14. Utformningen av artiklarna skiljer sig åt på några punkter, och vilken av dem som ska tillämpas beror på om personuppgifterna samlas in från den enskilde själv (artikel 13) eller från någon annan källa (artikel 14). En skillnad mellan artiklarnas krav är de möjligheter som finns enligt artikel 14 att underlåta att informera den registrerade i vissa situationer. En sådan undantagsmöjlighet är om informationsgivningen skulle visa sig vara omöjlig eller medför en oproportionerlig ansträngning (14.5 b). Några motsvarande eller liknande möjligheter att underlåta att informera finns inte direkt angivna i artikel 13. I förhållande till både artikel 13 och 14 är det dock möjligt att föreskriva undantag i nationell rätt i enlighet med artikel 23.

Utöver artikel 13, 14 och 23 innehåller dataskyddsförordning en annan bestämmelse som kan få betydelse för kraven på informationslämnande, nämligen artikel 11. Enligt artikeln ska den personuppgiftsansvarige inte vara skyldig att bevara, förvärva eller behandla information för att identifiera den registrerade endast i syfte att följa förordningen, om ändamålet med behandling i och för sig inte kräver identifiering.

¹⁶ Prop. 2011/12:45 s. 81 f.

Kan undantaget för bild- och ljudupptagningar behållas?

Det finns några olika sätt att motivera att nuvarande undantag från informationsplikten vid insamling genom ljud och bild kan behållas. Som redogjorts för ovan öppnar artikel 14 upp för att informationslämning kan underlåtas om personuppgifter samlas in från en annan källa än den enskilde själv. Att ingen sådan möjlighet finns då personuppgifter samlas in direkt från den enskilde enligt artikel 13 skulle kunna tolkas som att tillämpningen av artikel 13 förutsätter en direkt kontakt mellan den registrerade och den personuppgiftsansvarige, exempelvis muntligen eller skriftligen. Insamling genom bildupptagning där den personuppgiftsansvarige inte befinner sig i den registrerades omedelbara närhet, exempelvis för att insamlingen sker genom en övervakningskamera eller, som i Kustbevakningens fall, från ett flygplan, skulle då falla under artikel 14. I de flesta fall skulle då informationslämning till personer på bildupptagningen kunna bedömas som omöjlig eller i vart fall medföra en oproportionerlig ansträngning.

I det här avseendet har dock innebörden av artikel 13 och 14 tolkats på olika sätt.¹⁷ Att bedöma insamling av personuppgifter genom ljud och bild som insamlade från en annan källa än från den enskilde själv kan vara en tolkning som inte skulle stå sig vid en EU-rättslig prövning.

Om informationsskyldigheten ska bedömas utifrån artikel 13 finns, som sagt, istället möjligheten att göra undantag, om förutsättningar i artikel 23 kan anses uppfyllda. Det skulle i så fall, enligt vår mening, vara fråga om en inskränkning i syfte att skydda den registrerades rättigheter och friheter (artikel 23.1 i). Om den personuppgiftsansvarige skulle vara skyldig att efterforska identiteten på den som endast syns på en bild skulle detta riskera att bli ett integritetsintrång i sig. Genom identifieringen med namn etc. skulle ju personuppgiften bli sökbar på ett sätt som en bild aldrig kan vara. Själva efterforskningen kan ge personuppgiften spridning bland andra

¹⁷ Se redogörelsen i kommentaren till 23 § i Öman/Lindblom, Personuppgiftslagen, En kommentar, Zeteo, 2016. Som exempel ur redogörelsen kan nämnas att i prop. 2006/07:46 s. 86 f. anförs att endast personuppgifter insamlade genom någon form av direktkontakt med den enskilde är insamlade från denne själv. När det gäller personuppgifter insamlade genom kameraövervakning bedömer å andra sidan Datainspektionen att uppgifterna är insamlade från den enskilde själv, medan danska Datatilsynet dock verkar ha gjort en motsatt bedömning i liknande fall.

enskilda på ett sätt som riskerar att uppfattas som ett intrång, även om bilden kan framstå som helt harmlös. För att göra undantag enligt artikel 23 krävs, utöver att ett relevant syfte kan identifieras enligt 23.1, att den inskränkande lagstiftningen lever upp till kraven i artikel 23.2. Vi anser att kustbevakningsdatalagen får anses uppfylla dessa krav – en närmare genomgång görs längre fram i detta avsnitt.

Att efterforskning av en persons identitet kan vara ett integritetsintrång när behandlingen i övrigt inte kräver en sådan identifiering är samtidigt troligen ett av skälen bakom regleringen i artikel 11. Bestämmelsen i denna artikel ger ett självständigt stöd för att information till den enskilde kan underlåtas i situationer då denne i övrigt inte är direkt identifierad.

Enligt vår uppfattning bör man kunna se det förevarande undantaget från informationslämning antingen som en tillåten precisering av artikel 11 eller som ett tillåtet undantag i enlighet med artikel 23. Det är inte nödvändigt att i författningstexten ange vilken artikel undantaget grundar sig på. Oavsett vilken artikel som möjliggör undantaget anser vi att det bör göras ett tillägg till bestämmelsen som preciserar att undantaget avser situationer där en person inte är direkt identifierad. Att insamlingen sker genom ljud eller bild är inte i sig tillräckligt för att vare sig artikel 11 eller undantagsmöjligheterna i artikel 23 ska vara tillämpliga – det finns flera tänkbara situationer då insamling genom ljud eller bild kan ske på ett sådant sätt att information kan lämnas direkt till den registrerade, exempelvis om muntlig kommunikation med enskilda spelas in och bevaras.

Informationslämnande i larmsituationer

När det gäller information om personuppgiftsbehandling till den som larmar Kustbevakningen är syftet med bestämmelsen framför allt att de åtgärder som behöver vidtas med anledning av larmet inte ska försenas på ett sätt som kan äventyra deras effektivitet. Av bestämmelsen framgår att en prövning ska göras från fall till fall, vilket också framgår av förarbetsuttalandena. I larmsituationer där det kan vara befogat att underlåta att lämna information framstår det som självklart att det handlar om ett skyddsbehov, antingen för den registrerade själv, andra individer (exempelvis vid sjöräddning), allmän säkerhet eller något annat viktigt mål av generellt allmänt

intresse (exempelvis en miljöräddningsinsats). En inskränkning kan alltså göras i enlighet med artikel 23.1. Det kan anmärkas att det inledningsvis i artikel 23.1 också sägs att begränsningar enligt artikeln ska göras med respekt för andemeningen i de grundläggande rättigheterna och friheterna och utgöra en nödvändig och proportionell åtgärd i ett demokratiskt samhälle. Som vi anfört i våra allmänna överväganden bör man kunna utgå ifrån att författningar uppfyller sådana grundläggande krav (avsnitt 2.5.4).

För att vara tillåten måste inskränkande lagstiftning i enlighet med artikel 23 också uppfylla en rad andra krav som räknas upp i artikel 23.2.

Kraven enligt artikel 23.2 är tämligen svepande, särskilt i och med att artikeln inledningsvis anger att den nationella lagstiftningen ska uppfylla kraven ”åtminstone när så är relevant”. Vi menar att kustbevakningsdatalagen får anses nå upp till kraven i bestämmelsen. Lagen innehåller sådana bestämmelser som nämns i denna del av artikeln, bl.a. ändamålet med behandlingen, vilken myndighet som är personuppgiftsansvarig, bestämmelser som begränsar personuppgiftsbehandlingen på olika sätt och därmed utgör skyddsåtgärder. Den bestämmelse om lagringstid som finns i kustbevakningsdatalagen innebär ingen absolut tidsfrist, men är den reglering som ansetts relevant i sammanhanget. Att lagstiftningen som helhet innebär en avvägning mellan verksamhetens effektivitet och de registrerades relevanta fri- och rättigheter framgår av lagens syfte (1 kap. 1 §) och de överväganden som gjorts i lagstiftningsärendet. Den införda begränsningens omfattning är klart avgränsad.

Den registrerade kan inte ges rätt att bli informerad om den aktuella begränsningen, eftersom det skulle motverka syftet med den (punkten h).

3.5.7 Längsta tid för behandling

Förslag: Bestämmelserna i 5 kap. 7 § om gallring och bevarande för vissa ändamål samt om digital arkivering överförs till den nya kustbevakningsdatalagen. Formuleringar om att personuppgifter får bevaras för historiska, statistiska eller vetenskapliga ändamål ska anpassas till dataskyddsförordningens terminologi och därmed ändras till att avse arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål

Skälen för förslaget: Som vi redogjort för i våra allmänna överväganden (avsnitt 2.5.4) anser vi att bestämmelser som innehåller en uttrycklig bestämmelse om gallring är förenliga med dataskyddsförordningen, liksom bestämmelser om föreskriftsrätt. Bestämmelserna i 5 kap. 7 § i den nuvarande kustbevakningsdatalagen är alltså i huvudsak förenliga med dataskyddsförordningen och behöver inte ändras som en följd av att förordningen ska börja tillämpas. En justering bör dock göras av uttryckssättet i bestämmelsen när det gäller att uppgifter får bevaras för *historiska, statistiska eller vetenskapliga ändamål*. I dataskyddsförordningen används i stället i olika sammanhang uttryckssättet *arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål* (exempelvis i artikel 5.1 b och e). Vi bedömer inte att de olika uttrycken innebär någon skillnad i sak.¹⁸

Som vi redogjort för i våra allmänna överväganden anser Utredningen om 2016 års dataskyddsdirektiv att begreppet *gallring* bör utmönstras ur registerförfattningar. Vi menar att det kan finnas goda skäl för utredningens ställningstagande, men att det inte är motiverat att ändra de aktuella bestämmelserna om bevarande och gallring såvitt avser Kustbevakningens övriga operativa verksamhet, av följande skäl.

I propositionen till den nuvarande kustbevakningsdatalagen gjorde regeringen överväganden avseende behovet av gallringsbestämmelser. Där framhölls särskilt att gallringsbestämmelserna i kustbevakningsdatalagen är utformade i syfte att skydda den personliga integriteten. Vidare anfördes att gallringsbestämmelserna innebär att gallring ska utföras, alltså ska de uppgifter som omfattas av bestämmelserna heller inte arkiveras.¹⁹ Att ändra gallringsbestämmelsen i 5 kap. 7 § kustbevakningsdatalagen skulle innebära att utgångspunkten såvitt avser allmänna handlingar inte längre är gallring utan bevarande, låt vara inte i den operativa verksamheten, utan inom ramen för det arkivrättsliga regelverket. En sådan materiell förändring menar vi inte ligger inom ramen för vårt uppdrag. Vi föreslår därför bestämmelser i den nya kustbevakningsdatalagen som i sak överensstämmer med 5 kap. 7 § kustbevakningsdatalagen.

¹⁸ Jfr Ds 2017:28 s. 177 och 180 f. I promemorian lämnas en utförlig redogörelse för regleringen i 1995 års dataskyddsdirektiv och regleringen i dataskyddsförordningen, se s. 178–180.

¹⁹ Prop. 2011/12:45 s. 79 och 175.

3.5.8 En ny kustbevakningsdataförordning

Förslag: Bestämmelserna i 1, 4, 9, 10, 13 och 20 §§ i den nuvarande kustbevakningsdataförordningen förs över till en ny förordning med samma namn.

Skälen för förslaget: Kustbevakningsdatalagens förändrade tillämpningsområde innebär att bestämmelser i den nuvarande förordningen som rör den brottsbekämpande verksamheten inte ska tas upp i en ny kustbevakningsdataförordning. Det gäller 6, 7 och 14–18 §§ i förordningen.

Som vi tidigare redogjort för menar vi att 2 § i den nuvarande kustbevakningsdataförordningen reglerar samma förhållanden som också tas upp i dataskyddsförordningen. Bestämmelsen tillför inte heller något i sak som kan uppfattas som en precisering av dataskyddsförordningens bestämmelser. Den bör därför inte föras över till den nya kustbevakningsdataförordningen.

Övriga bestämmelser i kustbevakningsdataförordningen, som omfattas av dataskyddsförordningens tillämpningsområde, är däremot förenliga med förordningen. Vi gör bedömningen att av de bestämmelser som är förenliga med dataskyddsförordningen bör 1, 4, 9, 10, 13 och 20 §§ föras över till den nya förordningen. Resterade bestämmelser i kustbevakningsdataförordningen behövs inte längre i regleringen, av följande skäl.

Bestämmelsen i 8 § reglerar utlämnande på medium för automatiserad behandling. Med den nya utformningen av bestämmelsen om sådant utlämnande i kustbevakningsdatalagen blir paragrafen överflödig. Även 11 § hänvisar till den nuvarande lagregleringen av utlämnande på medium för automatiserad behandling och blir överflödig när lagregleringen får en ny utformning.

Utredningen om 2016 års dataskyddsdirektiv har gjort bedömningen att vissa bestämmelser om föreskriftsrätt som finns i förordningar som omfattas av deras utredningsuppdrag är överflödiga även av andra skäl än de ovan nämnda. Det gäller föreskriftsrätt avseende helt interna förhållanden hos de behöriga myndigheterna. Utredningen menar att myndigheternas interna

förhållanden kan och bör regleras på annat sätt än i föreskrifter.²⁰ Vi delar denna uppfattning och föreslår därför inga motsvarande bestämmelser i en ny kustbevakningsdataförordning. Bestämmelserna i den nuvarande förordningens 3, 5 och 19 §§ överförs därmed inte till den nya förordningen.

När det gäller bestämmelsen om föreskriftsrätt avseende bevarande för historiska, statistiska eller vetenskapliga ändamål (13 §) menar vi att uttryckssättet bör anpassas till dataskyddsförordningen, som i detta sammanhang talar om arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål (artikel 5.1 e).

Det kan slutligen anmärkas att när det gäller 4 § i den nuvarande kustbevakningsdataförordningen föreslås den paragrafen upphöra att gälla i kustbevakningens brottsdataförordning. Detta beror inte på att den är inaktuell, utan på att en generell reglering kommer att införas i brottsdataförordningen (4 b §).²¹ Utredningen om 2016 års dataskyddsdirektiv föreslår också att 20 § i kustbevakningsdataförordningen ska upphöra att gälla. Den regleringen ersätt dock av regleringen i 3 kap. 7 § brottsdatalagen. Vi menar att 20 § i förordningen fortfarande är relevant inom den nya kustbevakningsdataförordningens tillämpningsområde.²²

²⁰ SOU 2017:74 s. 376 f.

²¹ Se vidare författningsförslagen, SOU 2017:29 s. 261 och s. 294.

²² Även om föreskriftsrätten i många fall tas bort i enlighet med vad vi föreslår, kommer Kustbevakningen fortfarande ha en sådan rätt med avseende på direktåtkomst (10 § i nuvarande kustbevakningsdataförordningen och 4 § i vårt förslag).

4 Vapenlagen, vapenförordningen och förordningen om tillstånd till införsel av vissa farliga föremål

4.1 Vapenlagen och vapenförordningen

1.1.1 Om författningarna

Bakgrund

Den nuvarande vapenlagen (1996:67) och vapenförordningen (1996:70) är ett resultat av att den tidigare vapenlagen (1973:1176) behövde reformeras språkligt och systematiskt samt anpassas för att genomföra rådets direktiv om kontroll av förvärv och innehav av vapen (91/477/EEG). Några genomgripande materiella ändringar i den gällande regleringen avsågs dock inte, utom i de fall då det nämnda vapendirektivet krävde det. Departementschefen anförde följande:

Det råder i vårt land sedan lång tid tillbaka en allmän enighet om behovet av en sträng kontroll av innehav och bruk av skjutvapen och ammunition. Huvudsyftet med en sådan kontroll är att motverka missbruk av skjutvapen och att i möjligaste mån förhindra olycks-händelser i samband med hanteringen av sådana vapen. Av särskild betydelse är självfallet strävan att förhindra att vapen används i brottslig verksamhet.¹

I vapenlagen fanns från början ingen utförlig reglering av frågor om behandling av person- eller andra uppgifter i register. Att ett vapenregister skulle föras över tillståndspliktiga vapeninnehav och beslut enligt lagen framgick dock av 2 kap.17 §.²

¹ Prop. 1995/96:52 s. 26.

² Dåvarande 2 kap. 17 § upphävdes genom SFS 2014:591, prop. 2013/14:110.

År 1999 infördes fler bestämmelser om vapenregister i vapenlagen, bl.a. om vapenregistrens ändamål och en hänvisning till personuppgiftslagens reglering av rättelse och skadestånd.³ En redogörelse för den rättsliga regleringen och den praktiska hanteringen av vapenregistren finns i regeringens proposition (2013/14:110) En ny organisation för polisen.⁴ I samma proposition lämnas de förslag som numera utgör regleringen av personuppgiftsbehandling i vapenlagen. Skälen till förslagen var dels att den dåvarande regleringen ansågs komplex, dels att det låg i linje med den nya grundlagsbestämmelsen i 2 kap. 6 § regeringsformen att stärka enskildas integritetsskydd genom att införa uttryckliga bestämmelser om tillgång till personuppgifter och behandling av känsliga personuppgifter.⁵ Vidare ansågs det dåvarande regelverket, som bl.a. innebar både lokala och centrala vapenregister, hämma både en effektiv handläggning av vapenärenden och en effektiv brottsbekämpning.⁶

Kort om bestämmelserna om personuppgiftsbehandling i vapenlagen och -förordningen

Regleringen av personuppgiftsbehandlingen i vapenregister och vapenärenden finns i 1 a kap. vapenlagen och motsvarande kapitel i vapenförordningen. I lagen finns bestämmelser om personuppgiftsansvar, personuppgiftsombud, behandling av känsliga personuppgifter, tillgång till personuppgifter, rättelse och skadestånd samt innehållet i de fyra separata vapenregistren (vapeninnehavarregistret, vapenregistret, vapenhandlarregistret och registret över auktoriserade sammanslutningar för jakt- eller målskytte). För vapenregistren finns vidare bestämmelser om ändamål, bevarande och gallring och utlämnande av uppgifter ur registren.

I vapenförordningen finns bestämmelser om samkörning, tillgången till uppgifter och elektroniskt utlämnande.

³ SFS 1999:74, prop. 1998/99:36.

⁴ Prop. 2013/14:110 s. 483–488.

⁵ A. prop. s. 488.

⁶ A. prop. s. 493 f.

4.1.1 Kort om det nya vapendirektivet

I maj 2017 antogs ett direktiv med ändringar av det tidigare omnämnda vapendirektivet (Europaparlamentets och rådets direktiv (EU) 2017/853 av den 17 maj 2017 om ändring av rådets direktiv 91/477/EEG om kontroll av förvärv och innehav av vapen). En särskild utredare har fått i uppdrag att överväga hur ändringarna i vapendirektivet ska genomföras i svensk rätt.⁷ Ändringarna i vapendirektivet kan komma att innebära nya och förändrade bestämmelser i 1 a kap. vapenlagen. Vi anser inte att våra ställningstaganden påverkas av förändringarna i vapendirektivet i och för sig. De tillägg eller förändringar i 1 a kap. vapenlagen som behövs för att genomföra direktivet ingår i vapenutredningens uppdrag. Det kan anmärkas att i den mån direktivet ställer krav på en utökad personuppgiftsbehandling har denna behandling en unionsrättslig grund och är därmed förenlig med artikel 6 i dataskyddsförordningen (se vidare nedan).

4.1.2 Vilken EU-rättsakt är tillämplig?

Bedömning: Behandlingen av personuppgifter i vapenärenden och förändret av vapenregistren omfattas av dataskyddsförordningens tillämpningsområde.

Skälen för bedömningen: Bakom författningsregleringen av skjut- och andra vapen ligger, som framgår av det tidigare citatet ur vapenlagens förarbeten, den grundläggande synen att det behövs en sträng kontroll av innehav och bruk av vapen för att förhindra missbruk och olyckshändelser. Strävan att förhindra att vapen används i brottslig verksamhet är också, självfallet, ett viktigt syfte. Kontrollen av vapen bygger på att vapeninnehav är tillståndspliktigt. Handläggningen av vapenärenden kräver behandling av personuppgifter. Register över vem som fått tillstånd och för vilka vapen är vidare en grundläggande förutsättning för att tillståndskravet ska kunna upprätthållas på ett effektivt sätt, samtidigt som

⁷ Uppdrag att utreda vissa frågor på vapenlagstiftningens område (Ju 2017:E).

sådana register är en förutsättning för att kunna utreda och beivra brott med kopplingar till vapen.

Man skulle i och för sig kunna hävda att hela systemet med tillståndsplikt och registrering av innehavare, vapenhandlare och vapen har till syfte att förebygga brott och att förebygga hot mot den allmänna säkerheten. I så fall omfattas personuppgiftsbehandlingen inte av dataskyddsförordningens tillämpningsområde, utan av det nya dataskyddsdirektivets. Utredningen om 2016 års dataskyddsdirektiv har dock gjort en annan bedömning och menar att personuppgiftsbehandlingen i vapenärenden och vapenregister inte omfattas av det nya dataskyddsdirektivet.⁸ Brottdatalagen är därmed inte tillämplig på sådan behandling. I linje med denna bedömning ligger att personuppgiftsbehandlingen enligt vapenlagen i dag inte omfattas av polisdatalagen, polisens centrala registerförfattning avseende brottsbekämpande verksamhet. Även vår utgångspunkt är att personuppgiftsbehandlingen i vapenärenden och i vapenregistren omfattas av dataskyddsförordningens tillämpningsområde. Detta innebär att syftet med behandlingen inte är att bekämpa brott i det nya dataskyddsdirektivets mening, eller något annat av direktivets syften med behandlingen. Polismyndigheten är därmed inte heller att betrakta som en behörig myndighet i direktivets mening vid behandling i vapenärenden och i vapenregistren, eftersom uppgiften att ha hand om tillståndsprövning m.m. avseende vapen inte ingår i myndighetens brottsbekämpande uppdrag. De bestämmelser som reglerar registerföringen och behandlingen i registren, exempelvis för utlämnande, samt behandlingen i vapenärenden för att pröva frågor om tillstånd är alltså en reglering som måste vara förenlig med dataskyddsförordningen för att kunna behållas efter det att förordningen ska börja tillämpas.

Personuppgifter ur både vapenregistren och vapenärenden kan dock komma att användas i Polismyndighetens brottsbekämpande verksamhet. Utlämnande av uppgifter ur vapenregistren kan också ske till andra myndigheter med ett brottsbekämpande uppdrag och för sådana syften som omfattas av det nya dataskyddsdirektivet. Vi återkommer i nästa avsnitt till frågan hur man ska bedöma utlämnanden av personuppgifter ur vapenregistren och vapen-

⁸ SOU 2017:29 s. 254, s. 291 f., 308 och 697.

ärenden till brottsbekämpande verksamhet. Vi återkommer i avsnitt 4.1.5 med överväganden om det ska införas bestämmelser som klargör förhållandet mellan 1 a kap. vapenlagen och annan reglering av personuppgifter.

4.1.3 Överväganden om befintliga bestämmelser

Bedömning: Personuppgiftsbehandling i enlighet med 1 a kap. vapenlagen uppfyller kraven på rättslig grund i dataskyddsförordningens artikel 6.1 och 6.3.

Bestämmelser i 1 a kap. 1, 3–5, 7–15 §§ vapenlagen samt bestämmelserna i vapenförordningen är förenliga med dataskyddsförordningen och behöver inte ändras till följd av att förordningen ska börja tillämpas.

Bestämmelsen i 1 a kap. 2 om personuppgiftsombud är inte förenlig med dataskyddsförordningen. Bestämmelsen i 1 a kap. 6 § om rättelse och skadestånd måste ändras som en följd av att personuppgiftslagen upphör att gälla.

Skälen för förslaget och bedömningen:

Dataskyddsförordningens krav på rättslig grund

Som tidigare anförts är det grundläggande syftet med vapenlagstiftningen att vapeninnehav ska kunna kontrolleras så att generella risker med vapenanvändning, såsom olyckshändelser och brottslighet, ska kunna motverkas. Polismyndighetens uppdrag att pröva tillstånd till vapeninnehav får alltså betraktas som en uppgift av allmänt intresse. För att tillståndsplikten ska kunna upprätthållas på ett effektivt sätt krävs att personuppgifter behandlas vid tillståndsprövningen och att vapeninnehavare och vapenhandlare registreras. Personuppgiftsbehandlingen är alltså nödvändig för att utföra uppgiften av allmänt intresse och är därtill ett led i den myndighetsutövning som krävs för att upprätthålla tillståndskravet. Att föra vapenregistren och att handlägga vapenärenden är vidare en rättslig förpliktelse för Polismyndigheten. Det finns alltså rättsliga grunder för personuppgiftsbehandlingen i enlighet med dataskyddsförordningens artikel 6.1 c och e.

Tillståndsplikten för innehav av skjutvapen och handel med skjutvapen framgår av 2 kap. vapenlagen. Av 2 kap. 2 § följer att Polismyndigheten beslutar om tillstånd. Den uppgift av allmänt intresse som är grunden för personuppgiftsbehandlingen är alltså författningsreglerad, vilket innebär att förordningens krav på att den rättsliga grunden ska vara fastställd i nationell rätt (artikel 6.3) är uppfyllt. Förandet av vapenregistren är vidare författningsreglerat i 1 a kap. vapenlagen och i 1 a kap. i förordningen, vilket också bör kunna ses som en författningsreglering av den rättsliga grunden för personuppgiftsbehandlingen.

Medlemsstaterna är vidare förpliktade enligt unionsrätten att ha viss kontroll över vapeninnehav enligt rådets direktiv om kontroll av förvärv och innehav av vapen (91/477/EEG) (vapendirektivet). Medlemsstaterna är enligt direktivet bl.a. skyldiga att föreskriva om tillståndsplikt för vapeninnehav och handel med vapen. Medlemsstaterna ska också föra register över skjutvapen som ska innehålla bl.a. ägares namn. Den uppgift av allmänt intresse som gör det nödvändigt att behandla personuppgifter för tillståndsprövning och i vapenregister är alltså fastställd både i nationell rätt och i unionsrätten.

När det gäller rättsliga förpliktelser enligt artikel 6.1 c i dataskyddsförordningen ska syftet med behandlingen vara fastställt i nationell rätt eller unionsrätt enligt artikel 6.3. Ändamålet med vapenregistret anges i 1 a kap. 8 §. Att det övergripande syftet med att registrera vapeninnehav är att det ska gå att upprätthålla kontrollen av skjutvapen och den lagstadgade tillståndsplikten får vidare anses framgå av författningsregleringen som helhet och även av vapendirektivet.

Regleringen är i huvudsak förenlig med dataskyddsförordningen

Vapenlagen och -förordningen innehåller i huvudsak den typ av bestämmelser som utgör preciseringar av de grundläggande principerna för personuppgiftsbehandling och som vi tidigare konstaterat är förenliga med dataskyddsförordningen (jfr avsnitt 2.5.4), nämligen

- utseende av personuppgiftsansvarig (1 §)
- begränsning av tillgången till personuppgifter (5 §)

- precisering av vilka uppgifter som ska föras i register (7 §)
- registrens ändamål (8 §)
- bevarande och gallring (10 och 11 §§)
- utlämnande för statistiska ändamål (12 §)
- utlämnande till utländska myndigheter (13 §)
- direktåtkomst för svenska myndigheter (14 §)
- precisering av när samkörning får ske (1 och 2 §§ i förordningen)
- krav på särskild behörighet för tillgång och för viss behandling (3 och 4 §§ i förordningen)⁹
- elektroniskt utlämnande av uppgifter (5 § i förordningen)

När det gäller föreskriftsrätt finns sådana bestämmelser i 1 a kap. 15 § i lagen och 1 a kap 5 § i förordningen. Bestämmelser om föreskriftsrätt reglerar inte personuppgiftsbehandlingen som sådan. Bestämmelserna påverkas därmed inte av dataskyddsförordningen (se även avsnitt 2.5.4).

Behandling i registren eller i vapenärenden för att utlämna personuppgifter till brottsbekämpande verksamhet, polisens egen eller andra brottsbekämpande myndigheters, är att betrakta som en vidarebehandling som regleras i dataskyddsförordningens artikel 6.4. Av bestämmelsen i dataskyddsförordningen framgår att vidarebehandling kan regleras i nationell rätt och att det i sådana fall inte krävs att den personuppgiftsansvarige gör någon självständig bedömning av om ändamålet för vidarebehandling är förenligt med insamlingsändamålet (jfr skäl 50). Den nationella regleringen av vidarebehandling av uppgifter i vapenregistren för utlämnande till brottsbekämpande verksamhet finns i 1 a kap. 8 § vapenlagen, som anger vapenregistrens ändamål. Regleringen får anses uppfylla kraven i artikel 6.4, dvs. den är en nödvändig och proportionell åtgärd och skyddar ett av de mål som anges i artikel 23.1, nämligen det som tas upp i artikelns punkt d (bl.a. brottsbekämpning och

⁹ I 1 a kap. 4 § hänvisas till polisdatalagen (2010:361). Bestämmelsen bör ändras för att anpassas till kommande förändringar i polisdatalagen. Utredningen om 2016 års dataskyddsdirektiv lämnar förslag till denna följändring i SOU 2017:74 s. 114.

lagföring av brott). Om uppgifter i ett vapenärende ska lämnas ut finns däremot ingen särskild författningsreglering i 1 a kap. vapenlagen. Vi överväger frågor om sådant utlämnande under en särskild rubrik nedan.¹⁰

När det gäller ändamålsbestämmelser har vi, när det gäller kustbevakningsdatalagen, övervägt om det finns skäl för oss att föreslå ändringar som innebär bl.a. att begreppet *ändamål* inte längre ska användas i enlighet med de överväganden och förslag som lämnas av Utredningen om 2016 års dataskyddsdirektiv. Vi har valt att inte föreslå sådana förändringar i kustbevakningsdatalagens ändamålsbestämmelser och ser inte annorlunda på frågan när det gäller 1 a kap. 8 § vapenlagen. Se vidare våra överväganden i avsnitt 3.5.3.

Känsliga personuppgifter (1 a kap. 3 och 4 §§)

Regleringen av behandling av känsliga personuppgifter i 1 a kap. vapenlagen överensstämmer med vad som gäller enligt andra registerförfattningar för myndigheter som har både brottsbekämpande och andra uppdrag, exempelvis Kustbevakningen. Vi har tidigare konstaterat att denna utformning av regleringen får anses förenlig med dataskyddsförordningen i och för sig (se avsnitt 3.4). Vi återkommer i det följande med överväganden om regleringen ändå bör ändras i viss utsträckning.

Behandling av personnummer och uppgifter om lagöverträdelser

Vapenregistren innehåller personnummer. Detta är en självklar förutsättning för att personförväxling inte ska kunna förekomma när det gäller vapeninnehavare. Att vapenregistren innehåller personnummer framgår inte direkt av regleringen av registren, däremot framkommer det i bestämmelsen om bevarande i 1 kap. 10 § och av bestämmelser om vad en ansökan om vapeninnehav ska

¹⁰ Jfr även prop. 2009/10:85 s. 307 där det görs uttalanden om användandet av uppgifter i den brottsbekämpande verksamheten som härrör från polisens övriga verksamhet. Av uttalandet framgår att sådana utlämnanden ska bedömas utifrån den reglering som gäller för personuppgiftsbehandlingen i fråga – med andra ord personuppgiftslagen och i förekommande fall en registerförfattning. När dataskyddsförordningen börjar tillämpas förändras rättsläget på så sätt att bedömningen istället får göras på grundval av förordningen och i förekommande fall en registerförfattning.

innehålla (2 kap. 6 § vapenförordningen). Som framgår av våra allmänna överväganden finns en bestämmelse i dataskyddsförordningen som särskilt avser nationella identifikationsnummer – artikel 87. Av våra allmänna överväganden framgår också att det i viss mån är tveksamt vilka krav artikel 87 ställer på regleringen av personnummer. För det fall artikelns krav på skyddsåtgärder skulle anses tillämpligt på regleringen i vapenregistren, menar vi att detta krav får anses uppfyllt. Vapenregistrens författningsreglering får i sig anses innebära skyddsåtgärder eftersom den i olika avseenden avgränsar vilka register som förs, vad de innehåller, hur länge uppgifter bevaras och tillgången till uppgifter i registren. Användningen av uppgifter ur vapenregister och vapenärenden begränsas också av den tillämpliga sekretessregleringen (se vidare i det följande). Vidare kan anmärkas att behovet att använda personnummer är motiverat av att personer i registren kan identifieras på ett säkert sätt, vilket är förenligt med den reglering som föreslås i dataskyddslagen och som i sin tur av Dataskyddsutredningen bedömts förenlig med artikel 87.

I vapenärenden kan också förekomma behandling av uppgifter om fällande domar i brottmål. Att sådan behandling endast får ske under kontroll av en myndighet följer av artikel 10. När behandlingen utförs av en myndighet ställer artikeln inga övriga krav för att sådan behandling ska vara tillåten. Det kan ändå noteras att möjligheten att få ut uppgifter ur belastningsregistret i sig är författningsreglerad (lagen [1998:620] om belastningsregister) och att uppgifter om en enskilds personliga förhållanden i ärende enligt vapenlagen omfattas av sekretess, om det kan antas att den enskilde eller någon närstående till honom eller henne lider men om uppgiften röjs (35 kap. 23 § offentlighets- och sekretesslagen [2009:400]).

Personuppgiftsombud (1 a kap. 2 §)

Enligt 1 a kap. 2 § ska Polismyndigheten utse personuppgiftsombud. Begreppet *personuppgiftsombud* används i personuppgiftslagen och kommer att bli inaktuellt när denna lag upphävs. Skyldigheten att utse *dataskyddsombud* kommer att följa direkt av dataskyddsförordningen och bör därmed inte författningsregleras (se vidare avsnitt 2.5.7).

Rättelse och skadestånd (1 a kap. 6 §)

Enligt 1 a kap. 6 § vapenlagen tillämpas personuppgiftslagens bestämmelser om rättelse och skadestånd på motsvarande sätt vid behandling av personuppgifter enligt vapenlagen eller föreskrifter med stöd av lagen. Paragrafen måste ändras eftersom personuppgiftslagen kommer att upphöra att gälla. Vi återkommer i det följande med vår bedömning av om det behövs nya bestämmelser om rättelse eller skadestånd (avsnitt 4.1.5).

Bevarande och gallring (1 a kap. 9 §)

Som vi tidigare konstaterat (avsnitt 2.3.2) är det inte förenligt med dataskyddsförordningen att ha kvar bestämmelser som endast upprepar vad som redan följer av förordningen. Det kan ifrågasättas om bestämmelsen i 9 § är en sådan upprepning av förordningens princip om lagringsminimering (artikel 5.1 e) att den bör utgå. Vi menar dock att den får uppfattas som en precisering, eftersom den endast tar sikte på personuppgifter i vapenregistren och begränsar bevarandet i förhållande till vapenregistrens specifika ändamål. Den hänger också samman med bestämmelsen i 10 § och gör därmed reglering mer sammanhängande och begriplig (jfr dataskyddsförordningens skäl 8).

Vidarebehandling för syften som inte regleras i 1 a kap. vapenlagen

Ändamålsbestämmelserna i 1 a kap. 8 § vapenlagen ger endast stöd för behandling i vapenregistren för att ge information i brottsbekämpande verksamhet. I övrigt regleras utlämnande till svenska myndigheter genom bestämmelsen om direktåtkomst (14 §). Utlämnanden till andra myndigheter än de som fått direktåtkomst för andra syften än brottsbekämpning, liksom utlämnanden ur vapenärenden, får alltså bedömas utifrån det generellt tillämpliga regelverket om personuppgiftsbehandling, för närvarande personuppgiftslagen, samt tillämpliga sekretessbestämmelser.¹¹ Ett exempel på utlämnanden som i dag

¹¹ Jfr prop. 2009/10:85 s. 307. När det gäller uppgifter i vapenregister och vapenärenden är sådana sekretessbelagda om det inte står klart att uppgiften kan röjas utan fara för att vapen eller ammunition kommer till brottslig användning, 18 kap. 16 och 16 a §§. I vapenärenden regleras även sekretessen, som redogjorts för i texten ovan, i 35 kap. 23 §.

sker med tillämpning av finalitetsprincipen är att Kronofogdemyndigheten får uppgifter för tillgångsundersökningar enligt utsökningsbalken.¹² Kronofogdemyndigheten efterlyste i det senaste lagstiftningsärendet gällande vapenregistren att sekundära ändamål skulle införas i lagen. Regeringen anförde att det visserligen rent allmänt finns goda skäl att precisera tillåtna utlämnanden, men att det saknades beredningsunderlag i den delen och att frågan därför inte kunde behandlas vidare. Regeringen angav att det, utan närmare författningsreglering, är finalitetsprincipen som styr när uppgifter kan lämnas och till vem.¹³

Det ingår inte i vårt uppdrag att lämna förslag till författningsreglering som inte är nödvändig som en följd av EU:s dataskyddsreform. Vi saknar också möjlighet, inom ramen för vårt uppdrag, att tillräckligt utreda frågan om vilka sekundära ändamålsbestämmelser som skulle behövas. Vi kan dock konstatera att det inte finns något hinder mot att finalitetsprincipen tillämpas även efter det att personuppgiftslagen ersatts av dataskyddsförordningen. Det som tillkommer vid tillämpningen, och som är en nyhet i förhållande till det gamla dataskyddsdirektivet och personuppgiftslagen, är de särskilda omständigheter som ska beaktas vid bedömningen och som räknas upp i artikel 6.4 i förordningen. Om en vidarebehandling kan anses motiverad utifrån finalitetsprincipen behöver den personuppgiftsansvarige däremot inte göra någon ytterligare bedömning av om behandlingen är laglig enligt artikel 6.1 och 6.3. Detta framgår av förordningens skäl 50.

När det gäller tillämpningen av artikel 6.4 framgår det samtidigt, som vi tidigare redogjort för, att vidarebehandling som följer av nationell rätt är tillåten utan att en prövning görs med beaktande av artikelns punkter a–e. Man kan i det sammanhanget fråga sig om samverkansskyldigheten myndigheter emellan och uppgiftsskyldigheten i enlighet med 6 kap. 5 § offentlighets- och sekretesslagen kan anses vara en sådan nationell reglering som ersätter skyldigheten för en utlämnande myndighet att göra en självständig prövning av finalitetsprincipen, i de fall då det inte finns sekundära ändamålsbestämmelser som ger stöd för ett utlämnande. Frågan om förhållandet mellan finalitetsprincipen, 6 kap. 5 § offentlighets-

¹² 4 kap. 9 § utsökningsbalken, jfr Handbok, Utmätning, KFM 901, Utgåva 7, s. 72.

¹³ Prop. 2013/14:110 s. 497.

och sekretesslagen och sekundära ändamålsbestämmelser är inte ny. Det har i olika sammanhang hävdats att den lagreglering som 6 kap. 5 § offentlighets- och sekretesslagen utgör innebär att lagstiftaren redan tagit ställning till finalitetsprincipen och att en myndighet alltså inte behöver göra någon ytterligare prövning av den principen vid utlämnande till en annan myndighet som kan ske i enlighet med den bestämmelsen.¹⁴ Ett sådant resonemang överfört till dataskyddsförordningens kontext skulle innebära att lagregleringen i 6 kap. 5 § är en grund för vidarebehandling i nationell rätt som innebär att någon prövning i enlighet med artikel 6.4 inte skulle behöva göras. Samtidigt står dessa tidigare ställningstaganden om finalitetsprincipens tillämpning i förhållande till 6 kap. 5 § inte oemotsagda.¹⁵ När det gäller vårt uppdrag och regleringen av personuppgiftsbehandlingen i 1 a kap. vapenlagen, kan vi inte göra annat än att hänvisa till att regeringen tidigare angett att finalitetsprincipen ska tillämpas när utlämnanden som inte närmare regleras i 1 a kap. vapenlagen övervägs. Frågan om tillämpningen av finalitetsprincipen i enlighet med dataskyddsförordningens artikel 6.4 skulle dock förtjäna att bli mer övergripande belyst. Eftersom den frågan har en mycket vidare betydelse än med avseende på de författningar som ingår i vårt uppdrag, menar vi att det måste ske i ett annat sammanhang, exempelvis i den fortsatta beredningen av Informationshanteringsutredningens förslag till myndighetsdatalag.¹⁶

¹⁴ En redogörelse av olika uttalanden i denna fråga finns i Informationshanteringsutredningens betänkande *Myndighetsdatalag* (SOU 2015:39) s. 271–275. Informationshanteringsutredningens eget ställningstagande följer på s. 283 f. där det bl.a. anförs följande: ”När det gäller frågan om utlämnande av personuppgifter till andra myndigheter eller till enskilda är det alltså vår uppfattning att behandling i form av utlämnanden är förenliga med finalitetsprincipen så länge som utlämnandena som sådana sker i överensstämmelse med lag eller förordning enligt vilken uppgifterna får eller ska lämnas ut. Härmed avses i första hand utlämnanden till annan myndighet enligt 6 kap. 5 § OSL och utlämnanden av sekretessreglerade uppgifter till en annan myndighet eller enskild, på begäran eller på eget initiativ, som sker med stöd av någon sekretessbrytande bestämmelse. Vi menar alltså att lagstiftaren genom att reglera ett uppgiftslämnande får anses ha tagit ställning till att sådana utlämnanden som ska eller får ske inte är oförenliga med ursprungliga ändamål.”

¹⁵ Se föregående not.

¹⁶ SOU 2015:39.

4.1.4 Överväganden om och förslag till författningsändringar

Förslag: Bestämmelserna om utseende av personuppgiftsombud (1 a kap. 2 §) och rättelse och skadestånd (1 a kap. 6 §) upphävs. I 1 a kap. 2 § vapenlagen införs istället en upplysning om att 1 a kap. kompletterar dataskyddsförordningen och att dataskyddslagen är tillämplig på behandlingen enligt kapitlet.

Ordalydelsen i bestämmelserna om känsliga personuppgifter (1 a kap. 3 och 4 §§) anpassas till dataskyddsförordningens och brottsdatalagens reglering.

Bedömning: Ingen ny reglering av rättelse eller skadeståndsansvar behövs. Det saknas skäl att införa några författningsreglerade inskränkningar med avseende på artikel 16–21 i dataskyddsförordningen.

Skälen för förslaget och bedömningen:

Förhållandet till annan reglering av personuppgiftsbehandling

Vi har avseende andra författningar anfört att det finns skäl att införa en upplysande bestämmelse som avser bl.a. det förhållande att en författning kompletterar dataskyddsförordningen. Det gäller författningar som i dag innehåller en reglering av förhållandet mellan den aktuella författningen och personuppgiftslagen. I 1 a kap. vapenlagen finns dock ingen bestämmelse som anger hur regleringen förhåller sig till personuppgiftslagen. Vi anser att det nu finns skäl att i 1 a kap. vapenlagen införa bestämmelser som klargör att det är dataskyddsförordningen som är tillämplig på behandlingen i vapenregister och i vapenärenden. För myndigheter som har i uppdrag både att bekämpa brott och utföra andra förvaltningsuppgifter torde det finnas ett särskilt behov av att lagstiftningen är så tydlig som möjligt när det gäller vilket eller vilka nya regelverk som är tillämpliga i olika situationer.

Som vi konstaterat måste bestämmelserna i 2 § om personuppgiftsombud utgå. Vi föreslår att innehållet i 2 § ersätts av en ny bestämmelse som anger att 1 a kap. vapenlagen kompletterar dataskyddsförordningen och att dataskyddslagen därtill är tillämplig (se vidare våra allmänna överväganden, avsnitt 2.5.9, om hur förhållandet till dataskyddslagen bör formuleras.)

Anpassning av bestämmelserna om känsliga personuppgifter

Som vi anfört tidigare i detta kapitel (avsnitt 4.1.4) är de nuvarande bestämmelserna om känsliga personuppgifter i och för sig förenliga med dataskyddsförordningen. Begreppet *känsliga personuppgifter* kommer dock, både i dataskyddslagen och i brottsdatalagen, få en vidare räckvidd än dagens begrepp. En justering bör därför göras så att samtliga de kategorier som omfattas av begreppet enligt dataskyddslagen och brottsdatalagen omfattas. Detta kan lämpligen åstadkommas genom att dagens uppräkningslista av personuppgifter som avses tas bort och ersätts med en hänvisning till den uppräkningslista som görs i 9.1 dataskyddsförordningen (jfr 3 kap. 1 § dataskyddslagen).

När det gäller förutsättningarna i sak för att behandla känsliga personuppgifter har vi när det gäller kustbevakningsdatalagen (se avsnitt 3.5.4) konstaterat att det finns tre olika möjligheter som alla är förenliga med dataskyddsförordningen – att behålla bestämmelserna oförändrade, att ta bort dem och låta dataskyddslagens reglering bli gällande eller att anpassa dem till vad som kommer att gälla enligt brottsdatalagen. Vi bedömer att det inte är någon större saklig skillnad mellan de tre alternativen. Det som bör vara utslagsgivande är vilken konstruktion som kan anses underlättat för tillämparen. Polismyndigheten är, liksom Kustbevakningen, en myndighet som kommer att ha att förhålla sig till flera olika regelverk om dataskydd, varav tre olika generella regleringar, nämligen brottsdatalagen, dataskyddsförordningen och dataskyddslagen. Vi menar att om regleringen så långt det är möjligt blir likalydande för myndigheten måste detta vara något som underlättar vid tillämpningen. Just när det gäller känsliga personuppgifter finns det en möjlighet att inom det område som i och för sig övergripande regleras av dataskyddsförordningen ha en reglering som överensstämmer med den som kommer att gälla inom brottsdatalagens tillämpningsområde. Vi föreslår därför att regleringen av förutsättningarna för att behandla känsliga personuppgifter och sökbegränsningar avseende sådana personuppgifter anpassas så att de överensstämmer med brottsdatalagens.

Rättelse och skadestånd

Vi anser att dataskyddsförordningens bestämmelser om rättelse och skadestånd blir tillämpliga även om ingen särskild hänvisning görs i registerförfattningar, se vidare avsnitt 2.5.9. Den nuvarande bestämmelsen i 1 kap. 6 § vapenlagen kan alltså utgå och paragrafen upphävas.

Särskilt om begreppet gallring i 1 a kap. 11 §

Som vi tidigare redogjort för har Utredningen om 2016 års dataskyddsdirektiv väckt frågan om inte bestämmelser som använder ordet *gallring* bör ändras i vissa fall. När det gäller regelrätta register menar vi att det dock kan finnas skäl att ha kvar bestämmelser om gallring, när syftet med bestämmelsen är att ge förutsättningar för just en arkivrättslig gallring. Att syftet samtidigt är att skydda den enskildes integritet motiverar i sådana fall inte att terminologin förändras, se vidare våra överväganden om gallringsbestämmelserna i belastningsregistret (avsnitt 5.5).

I 1 a kap. vapenlagen finns en bestämmelse som tar upp gallring – det gäller gallring av uppgifter om hemvärnets personal i 11 §. Av förarbetsuttalanden framgår att bestämmelsen har flera syften, varav ett är att ge förutsättningar just för en arkivrättslig gallring – det sägs i propositionen att uppgifterna inte ska bevaras för historiska, vetenskapliga eller statistiska ändamål (i vart fall inte inom ramen för arkivering utförd av Polismyndigheten).¹⁷ Som framgår av propositionen var frågan om användningen av ordet gallring redan väckt i det lagstiftningsarbetet genom Riksarkivets remissyttrande. Vi menar att det inte finns skäl att nu ändra bestämmelsen om gallring i 1 a kap. 11 §.¹⁸

¹⁷ Prop. 2013/14:110 s. 501–502.

¹⁸ A. prop. s. 501.

Den enskildes rättigheter enligt förordningen – behov av inskränkningar?

Som tidigare redogjorts för innehåller dataskyddsförordningen direkt tillämpliga rättigheter för den enskilde med avseende på information, rättelse m.m. Eftersom rättigheterna i viss mån avviker från vad som gäller i dag enligt personuppgiftslagen anser vi att det bör övervägas vad förordningens bestämmelser innebär i praktiken för behandlingen i vapenärenden och vapenregistren och om några inskränkningar behöver göras enligt artikel 23.

Våra generella överväganden om enskildas rättigheter följer av avsnitt 2.5.8. Vi har kommit fram till att det i allmänhet inte är motiverat att införa inskränkningar i den registrerades rättigheter enligt förordningen. Vi har inte funnit några skäl som mer specifikt rör behandlingen av personuppgifter enligt 1 a kap. vapenlagen som leder till något annat ställningstagande.

4.2 Förordningen om tillstånd till införsel av vissa farliga föremål

4.2.1 Om författningen

Bakgrund

Förordningen (1990:415) om tillstånd till införsel av vissa farliga föremål (kallas *förordningen om farliga föremål* eller *förordningen i det följande*) innebär i princip ett införselförbud för föremål som inte är skjutvapen men som är ägnade att användas som vapen eller tillhyggen vid våldsutövning mot andra människor, exempelvis springstiletter och knogjärn.

Förordningen ska ses mot bakgrund av införandet av lagen (1988:254) om förbud beträffande knivar och andra farliga föremål (knivlagen). Genom knivlagen infördes förbud mot att inneha knivar, andra stick- och skärvapen och andra föremål som är ägnade att användas som vapen vid brott mot liv eller hälsa. Förbudet var först begränsat till att avse allmänna sammankomster och offentliga tillställningar. Redan två år efter ikraftträdandet utvidgades för-

budet till att avse allmän plats och inom skolområden.¹⁹ Ett utvidgat knivförbud ansågs vara ägnat att minska antalet våldsbrott med stick- och skärvapen och andra liknande tillhyggen.

När det gällde förbud mot saluförande och införsel av knivar m.m. anförde departementschefen följande.

Som utredningen anför måste en verksamhet som syftar till saluhållning av föremål som endast kan användas för våld mot andra människor anses som stötande. Samhällets avståndstagande mot sådana förfaranden bör tydligt markeras. Jag delar därför utredningens uppfattning att det bör införas ett förbud mot att bjuda ut gatustridsvapen till försäljning.

[...]

När det därefter gäller frågan om ett införselförbud för gatustridsvapen delar jag i och för sig utredningens uppfattning att det inte heller finns skäl att tillåta import av sådana.²⁰

Ett förbud mot saluhållning av vissa farliga föremål infördes i knivlagen. Av framförallt författningstekniska skäl infördes dock inget införsel förbud i lagen, utan regleringen infördes istället i förordning. Föreskriftsrätten följde av dåvarande vapenlagen (1973:1176), 1 § tredje stycket (jfr nuvarande 11 kap. 1 § a).²¹

¹⁹ SFS 1990:413, prop. 1989/90:129.

²⁰ A. prop. s. 17.

²¹ Se vidare a. prop. s. 17 f.

Förordningens innehåll

Förordningen om farliga föremål omfattar sju paragrafer. Enligt förordningen krävs tillstånd för att föra in vissa särskilt uppräknade farliga föremål, exempelvis springstiletter och knogjärn. Förutsättningen för tillstånd är att den som vill föra in föremålet i fråga kan visa att det är avsett att ingå i en vapensamling eller innehas för något liknande ändamål. Polismyndigheten prövar frågor om tillstånd.

Den bestämmelse i förordningen som berör personuppgiftsbehandling är 4 §, som anger att vissa bestämmelser i vapenlagen ska gälla ”i tillämpliga delar”. Till de uppräknade bestämmelserna hör 1 a kap. 7 §, som reglerar förandet av vapenregister och registrens innehåll. Polismyndigheten ska alltså föra ett register över personer som beviljas tillstånd att föra in ett sådant farligt föremål som omfattas av förordningens tillämpningsområde.

4.2.2 Överväganden och förslag

Bedömning: Personuppgiftsbehandling i enlighet med förordningen om farliga föremål omfattas av dataskyddsförordningens tillämpningsområde. Personuppgiftsbehandlingen har en rättslig grund i enlighet med dataskyddsförordningens artikel 6.1 och 6.3.

Förslag: I förordningen införs två nya hänvisningar, till 1 a kap. 2 § och 8 §§ vapenlagen.

Skälen för bedömningen och förslaget: Liksom när det gäller vapenlagen och personuppgiftsbehandling i vapenärenden och i vapenregistren skulle man kunna se personuppgiftsbehandling med anledning av införselförbudet av farliga föremål som en verksamhet som syftar till att förebygga brott och hot mot den allmänna säkerheten, i vart fall i vid bemärkelse. Som vi anført gällande vapenlagen m.m. (se avsnitt 4.1.3) har vi dock som utgångspunkt de ställningstaganden som Utredningen om 2016 års dataskyddsdirektiv har gjort när det gäller gränsdragningen för det nya dataskyddsdirektivet. Behandling av personuppgifter med anled-

ning av förordningen om farliga föremål bör betraktas på samma sätt som hanteringen av vapenärenden. Personuppgiftsbehandling som utförs i enlighet med förordningen om farliga föremål omfattas alltså av dataskyddsförordningens tillämpningsområde.

Eftersom Polismyndigheten getts i uppdrag att upprätthålla införselförbudet av farliga föremål genom att ge tillstånd och även registrera innehav av sådana föremål, får personuppgiftsbehandlingen anses vara nödvändig för att fullgöra en uppgift av allmänt intresse i enlighet med dataskyddsförordningens artikel 6.1 e. Uppgiften av allmänt intresse, och även personuppgiftsbehandlingen till viss del, är reglerad i författning och därmed är också kravet på rättslig grund enligt artikel 6.3 uppfyllt. Det kan tilläggas att allmänintresset i att ha ett införselförbud för farliga föremål tydligt framgår om man ser regleringen i sitt sammanhang, tillsammans med vapenlagen, knivlagen och förarbetena till dessa lagar.

Förutom hänvisningen till bestämmelsen om vapenregister i vapenlagen innehåller förordningen om farliga föremål ingen närmare reglering av personuppgiftsbehandling. Dataskyddsförordningen innebär i sig inga krav på att personuppgiftsbehandling ska särregleras enligt nationell rätt. Dataskyddsförordningens bestämmelser är direkt tillämpliga på behandlingen oavsett om det finns nationell rätt som preciserar principerna i förordningen eller inte.

Som vi tidigare anfört ligger det inte inom ramen för vårt uppdrag att föreslå nya materiella bestämmelser om personuppgiftsbehandling. Vi har däremot när det gäller flera författningar föreslagit att det ska införas vad som får betraktas som i huvudsak upplysande bestämmelser, för att klargöra förhållandet mellan en registerförfattning och annan reglering. Det kan i och för sig ifrågasättas om sådana hänvisningar är nödvändiga i alla författningar. När det gäller förordningen om farliga föremål anser vi dock att den, genom hänvisningarna till vapenlagen och genom sitt innehåll och syfte i övrigt, har ett sådant samband med vapenlagstiftningen att det kan vara lämpligt att i förordningen hänvisa inte bara till 1 a kap. 7 § utan också till den bestämmelse som vi föreslår ska införas 1 a kap 2 §. Bestämmelsen är till för att klargöra förhållandet att det är dataskyddsförordningen som är tillämplig på personuppgiftsbehandlingen enligt förordningen om farliga föremål. Vi anser vidare att en hänvisning till 1 a kap. 8 § bör

införas. Uppgifterna om innehav av farliga föremål skulle kunna behövas för att utreda brott etc. En sådan vidarebehandling torde i och för sig vara tillåten med en tillämpning av den bedömningsmodell som föreskrivs i 6.4 dataskyddsförordningen. Som vi utvecklat i avsnitt 4.1.4 kan dock nationell författningsreglering ersätta den prövning som föreskrivs i artikel 6.4, vilket torde underlätta för tillämparen. En hänvisning till 1 a kap. 8 § innebär att vidarebehandling i brottsbekämpande syften får anses följa av nationell rätt på det sätt som förutsätts i artikel 6.4.

5 Lagen och förordningen om belastningsregister

5.1 Om författningarna

Bakgrund

Den nuvarande lagen (1998:620) och förordningen (1999:1134) om belastningsregister är en del av den reformerade lagstiftning om polisens register som genomfördes 1998 efter förslag av Registerutredningen.¹ En utgångspunkt för lagstiftningsarbetet var att uppgifter om påföljder och uppgifter om misstankar om brott ska hållas åtskilda och inte behandlas inom samma register. Det övergripande syftet med belastningsregistret ansågs dock vara detsamma som tidigare, nämligen att olika myndigheter, framför allt de brottsbekämpande och rättsvårdande myndigheterna, på ett enkelt sätt ska få tillgång till de uppgifter som behövs i verksamheten. När det gällde vilka uppgifter som ska få registreras och i vilka situationer uppgifterna ska få utlämnas innebar den nya regleringen inga större förändringar i förhållande till lagen (1963:197) om allmänt kriminalregister.

¹ I Registerutredningens uppdrag ingick att lämna förslag till en rättslig reglering av belastningsregistret och misstankeregistret samt överväga vilka ändringar som behövdes i polisregisterlagen (1965:94) samt att lämna förslag till en rättslig reglering av polisundermåttregister och DNA-register. I propositionen (1997/98:97) *Polisens register* föreslog regeringen bl.a. lagar om belastnings- och misstankeregister samt en polisdatalog (SFS 1998:622).

Kort om författningarnas innehåll

I lagen om belastningsregister föreskrivs en skyldighet för Polismyndigheten att med hjälp av automatiserad behandling föra ett belastningsregister som myndigheten är personuppgiftsansvarig för (1 §). Lagen innehåller sedan till största delen bestämmelser om belastningsregistrets innehåll (3–5 §§), utlämnande av uppgifter ur registret (6–15 §§) och gallring (16–18 §§). Regeringen har möjlighet att meddela närmare föreskrifter och förordningen om belastningsregister innehåller också mer detaljerade bestämmelser på dessa områden.

Inledningsvis i lagen finns bestämmelser om belastningsregistrets ändamål (2 §) och om förhållandet till andra lagar (personuppgiftslagen [1998:204] och lagen [2013:329] med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen, 1 a § respektive 1 b §).

När det gäller rättigheter för den registrerade innehåller lagen dels bestämmelser om rätt till utdrag från registret till den registrerade själv, dels en hänvisning till personuppgiftslagens bestämmelser om rättelse och skadestånd (9 § respektive 20 §).

Utbyte inom EU av uppgifter ur medlemsstaternas kriminalregister

Genom rådets rambeslut 2009/315/RIF om medlemsstaternas utbyte av uppgifter ur kriminalregistret och uppgifternas innehåll (kallas *rambeslutet om kriminalregister* eller *rambeslutet* i det följande) skapades nya förbättrade möjligheter för medlemsstaterna att rutinmässigt utbyta uppgifter ur de nationella kriminalregistren. Rambeslutet innebär en skyldighet att fortlöpande informera det land där en dömd person är medborgare om domar som meddelas i en annan medlemsstat. Sådana uppgifter ska registreras i medborgarstaten. På detta sätt ska kriminalregistret i den stat där en person är medborgare täcka in uppgifter från alla EU-länder. Som påpekas i förarbetena skedde även före genomförandet av rambeslutet ett liknande informationsutbyte, men rambeslutet kräver ett något annorlunda och snabbare förfarande.²

² Prop. 2011/12:163 s. 55.

Rambeslutet om kriminalregister innehåller också bestämmelser om utbyte av uppgifter efter särskild begäran från en medlemsstat. Bestämmelserna innebär en förenkling, genom att varje medlemsstat har utsett en centralmyndighet som administrerar uppgiftslämnandet. Rambeslutet gör skillnad på om begäran sker i syfte att använda uppgifterna i ett brottmålsförfarande eller om det sker för andra ändamål. Medlemsstaterna har möjlighet att begränsa åtkomsten till uppgifter i andra syften än brottmålsförfaranden. Vid genomförandet ansåg regeringen att det var rimligt att ge andra medlemsstaters myndigheter, vars verksamhet med exempelvis tillståndsprövning motsvarar svenska myndigheters, tillgång till uppgifter ur belastningsregistret.³

Rambeslutet har genomförts i svensk rätt i huvudsak genom tillägg i lagen och förordningen om belastningsregister.⁴

Tillämpliga sekretessbestämmelser

För uppgifter i belastningsregistret råder absolut sekretess. Uppgifter får inte lämnas ut utom i de fall som regleras i lagen om belastningsregister och i säkerhetsskyddslagen (1996:627) samt i förordningar som har meddelats med stöd av dessa lagar (35 kap. 3 § offentlighets- och sekretesslagen [2009:400]). Den absoluta sekretessen gäller dock bara i verksamhet som avser förande av eller uttag ur registret. När uppgifter tas ut av en myndighet för att användas i den egna verksamheten gäller istället i förekommande fall sekretess enligt de bestämmelser som gäller för denna verksamhet. Enskilda som fått uppgifter ur belastningsregistret avseende någon annan än dem själva är istället bundna av tystnadsplikt (19 §).

³ Prop. 2011/12:163 s. 42 f.

⁴ SFS 2012:762 och prop. 2011/12:163.

5.2 Vilken EU-rättsakt är tillämplig?

Bedömning: Förändret av belastningsregistret och uttag ur registret i brottsbekämpande syften faller under det nya dataskyddsdirektivets tillämpningsområde. På annan behandling av personuppgifter i registret, exempelvis för att lämna belastningsuppgifter som underlag för olika slag av lämplighets- och tillståndsprövningar, tillämpas dataskyddsförordningen.

Skälen för bedömningen:

Dataskyddsdirektivet, dataskyddsförordningen eller båda?

Belastningsregistret är ett helt automatiserat register som innehåller personuppgifter. Förändret av belastningsregistret och behandling av uppgifter i registret, exempelvis sökning och utlämnande, innefattar alltså sådan personuppgiftsbehandling som kan falla antingen under dataskyddsförordningens eller det nya dataskyddsdirektivets tillämpningsområde. Det kan dock vara värt att notera att bestämmelser om uttag ur registret i och för sig inte tar sikte på att reglera frågor om dataskydd, utan är nödvändiga för att bryta den absoluta sekretess som råder för registret och som beskrivits ovan (avsnitt 5.1). Eftersom det dels är fråga om ett regelrätt register, dels om ett helt automatiserat sådant, kommer varje utlämnande som aktualiseras utifrån de sekretessbrytande bestämmelserna dock att innebära även att personuppgifter behandlas på sätt som omfattas av de dataskyddsrättsliga regelverken (jfr vidare våra allmänna överväganden, avsnitt 2.5.4).

Belastningsregistret förs av en myndighet som har ett brottsbekämpande uppdrag i det nya dataskyddsdirektivets mening.⁵ Belastningsregistret innehåller uppgifter om begångna brott och i påföljder för brott. Det innehåller också uppgifter om kontaktförbud, förbud enligt 3 kap. 5 § lagen (2015:642) om europeisk skyddsorder och tillträdesförbud. Personuppgiftsbehandling

⁵ Enligt artikel 3.7 är definitionen av en *behörig myndighet* bl.a. en offentlig myndighet som har behörighet att förebygga, förhindra, utreda eller avslöja brott. Endast behöriga myndigheters personuppgiftsbehandling i brottsbekämpande syften omfattas av direktivets tillämpningsområde, se artikel 2.

avseende frågor om att meddela tillträdes- och kontaktförbud får anses omfattas av det nya dataskyddsdirektivets tillämpningsområde i och för sig, eftersom förbuden syftar till att beivra brott. Även en europeisk skyddsorder bör betraktas på samma sätt, eftersom sådana avser kontaktförbudsliknande skyddsåtgärder som har meddelats i en medlemsstat i EU och ska erkännas och verkställas i en annan medlemsstat. Lagen om europeisk skyddsorder genomför ett EU-direktiv.⁶ Att uppgifter om en europeisk skyddsorder förs in i belastningsregistret kan alltså jämföras med att en uppgift om ett kontaktförbud registreras där.

Avgörande för vilken EU-rättsakt som är tillämplig är dock inte uppgiftens karaktär eller innehåll i och för sig. Att den myndighet som utför behandlingen har ett brottsbekämpande uppdrag är en förutsättning för att det nya dataskyddsdirektivet ska vara tillämpligt, men utöver detta måste också syftet med behandlingen vara att bekämpa brott eller något annat av de syften som anges i artikel 1.1 i direktivet.

Som redan redogjorts för anges i lagen att belastningsregistret har flera ändamål, varav vissa uttryckligen avser brottsbekämpning och lagföring av brott (2 § första stycket 1–3), medan det är mer ovisst hur man ska se på syftet med att tillhandahålla belastningsuppgifter för tillstånds- och lämplighetsprövningar m.m. (2 § första stycket 4). Det går alltså inte utan vidare att säga att samtliga angivna ändamål i 2 § är sådana som omfattas av det nya dataskyddsdirektivets tillämpningsområde eller av dataskyddsförordningens. För analysen av vilken EU-rättsakt som är tillämplig har vi utgått ifrån att personuppgiftsbehandling i registret kan delas upp i två delar. Den ena avser förandet av registret, dvs. den behandling som behövs för att lägga in personuppgifter i registret och sedan bevara dem där. Den andra är sökningar i och uttag ur registret, som alltså görs för att informationen i registret behövs både i brottsbekämpande myndigheters verksamhet och i annan verksamhet, i huvudsak för olika tillstånds- och lämplighetsprövningar som görs både av Polismyndigheten och av andra myndigheter.

Innan vi kommer in på frågan om uttag ur registret överväger vi hur man ska se på förandet av registret. Denna fråga är central,

⁶ Se vidare prop. 2014/15:139.

eftersom den övergripande EU-rättsakt som är tillämplig på förandet av registret innehåller de grundläggande kraven på personuppgifternas behandling; deras riktighet, den enskildes rätt till registerutdrag, bevarande av uppgifterna m.m.

Vi menar att förandet av registret får anses ske för de syften som anges i 2 § första stycket 1–3 lagen om belastningsregister. Dessa syften är sådana som omfattas av det nya dataskyddsdirektivets tillämpningsområde, nämligen att bekämpa och lagföra brott och verkställa straffrättsliga påföljder.⁷ Att utlämnande av uppgifter ur registret eventuellt kan komma att ske även för andra ändamål, såsom olika lämplighetsbedömningar (2 § första stycket 4), påverkar inte frågan om registrets grundläggande ändamål. Den behandling av personuppgifter det innebär att samla in uppgifterna och bevara dem i registret omfattas alltså av det nya dataskyddsdirektivets tillämpningsområde. När uppgifter sedan söks fram och i förekommande fall utlämnas för något av de ändamål som anges i 2 § första stycket 1–3 är det nya dataskyddsdirektivet också tillämpligt.

Frågan är då hur man ska se på uttag ur registret när det gäller att ge information om brottslig belastning som underlag för olika tillstånds- och lämplighetsprövningar. Utredningen om 2016 års dataskyddsdirektiv anser att behandling i belastningsregistret för sådana ändamål i huvudsak inte kan betraktas som brottsbekämpande i direktivets mening.⁸ Regeringen har å andra sidan gett uttryck för att behandling av uppgifter ur belastningsregistret vid tillståndsgivning eller i ett anställningsförfarande har som ändamål att i vid mening förebygga brott.⁹ Om ett sådant synsätt tillämpas skulle i princip samtliga behandlingar i belastningsregistret, både förandet av det, sökningar och uttag för utlämnanden, falla inom det nya dataskyddsdirektivets tillämpningsområde. Den generella reglering som då skulle bli tillämplig på personuppgiftsbehandlingen i belastningsregistret skulle vara enbart brottsdatalagen (som kommer att genomföra det nya dataskyddsdirektivet i svensk rätt, se avsnitt 2.3.4). En sådan

⁷ Jfr Europarådets rekommendation nr R(84)10 om kriminalregister och återanpassning av personer som dömts för brott.

⁸ SOU 2017:29 s. 216.

⁹ Prop. 2011/12:163 s. 50.

ordning skulle onekligen underlätta för Polismyndigheten som personuppgiftsansvarig.

Frågan om det nya dataskyddsdirektivets närmare gränsdragning är komplex. Vi menar att det i och för sig inte framstår som omöjligt att i vissa avseenden ha en något vidare syn på det nya dataskyddsdirektivets tillämpningsområde än Utredningen om 2016 års dataskyddsdirektiv haft, exempelvis när det gäller belastningsregistret. Samtidigt har vi inte haft möjlighet att inom ramen för vårt uppdrag göra samma heltäckande analys av direktivets tillämpningsområde som utredningen har gjort. Denna analys faller ju också tydligt inom den utredningens uppdrag. Våra överväganden och våra förslag utgår därför från de slutsatser som utredningen dragit. Det slutliga ställningstagandet om det nya dataskyddsdirektivets tillämpningsområde får göras inom ramen för det fortsatta lagstiftningsarbetet. Skulle man då göra bedömningen att dataskyddsförordningen inte alls ska tillämpas på personuppgiftsbehandlingen i belastningsregistret får våra författningsförslag anpassas därefter. Våra överväganden torde vara tillräckligt beredningsunderlag för att det ska gå att göra en sådan justering.

Vilken behandling omfattas av dataskyddsförordningen respektive det nya dataskyddsdirektivet?

Som redan berörts är sökningar och i förekommande fall utlämnanden av uppgifter enligt 2 § första stycket 1–3 sådan behandling för syften som omfattas av det nya dataskyddsdirektivets tillämpningsområde. Sökningar enligt 2 § första stycket 4 avser däremot i flertalet fall utlämnanden vars syfte inte är brottsbekämpning etc.

Utöver 2 § finns det, som redan nämnts, flera bestämmelser både i lagen och i förordningen som reglerar frågor om utlämnanden mer i detalj. Med ledning av författningstexten kan det i många fall avgöras om det är det nya dataskyddsdirektivet eller dataskyddsförordningen som är tillämplig. I andra fall är regleringen generell på ett sätt som gör att en bedömning får göras från fall till fall. Vi gör nedan en så noggrann genomgång som vi anser vara möjlig med utgångspunkt från författningsregleringen och det

synsätt på det nya dataskyddsdirektivets tillämpningsområde som Utredningen om 2016 års dataskyddsdirektiv redovisar.

För Polismyndighetens sökningar i registret för ändamål som anges i 2 § första stycket 1 gäller alltså det nya dataskyddsdirektivet. Även när det gäller behandling för utlämnande (oavsett om det sker genom direktåtkomst, se 19 § i förordningen, eller inte) till Skatteverket, Tullverket, Kustbevakningen, åklagarmyndigheten eller allmän domstol för ändamål i 2 § första stycket 1–3 (själva utlämnandet regleras i 6 § första stycket 2) blir direktivet tillämpligt. Utlämnande för tillsynsverksamhet som utförs av bl.a. riksdagens ombudsmän omfattas däremot inte av det nya dataskyddsdirektivet (6 § första stycket 1). När det gäller utlämnanden till förvaltningsdomstol (6 § första stycket 3) beror det på vad prövningen i förvaltningsdomstolen gäller. Enligt bestämmelsens hänvisning till 2 § handlar det om tillstånds- eller lämplighetsprövningar, men det kan också gälla andra frågor som regleras av författning. Som framgår av vår genomgång i det följande kan vissa sådana frågor falla inom det nya dataskyddsdirektivets tillämpningsområde, i huvudsak frågor som uppstår hos behöriga myndigheter avseende verkställighet av straff.

För svenska myndigheters tillgång, utöver vad som behandlats ovan, gäller alltså enligt 6 § första stycket 4 att utlämnande sker i den utsträckning det är särskilt föreskrivet. Sådana föreskrifter finns i förordningens bestämmelser i 10–18 §§ och 20 §. Av författningstexten framgår att utlämnanden enligt 11–18 och 20 §§ görs till myndigheter som inte har ett brottsbekämpande uppdrag och där ärendet i vilket uppgifterna ur belastningsregistret behövs inte omfattas av det nya dataskyddsdirektivets tillämpningsområden. Detsamma gäller för 10 §, men med några undantag:

- utlämnande till regeringen (föredragande statsråd eller den statsrådet bemyndigar) i ärenden om utlämning för brott, nåd i brottmål, i ärenden om överförande av straffverkställighet enligt lagen (1972:260) om internationellt samarbete rörande verkställighet av brottmålsdom (delar av 10 § första stycket 1),¹⁰

¹⁰ SOU 2017:29 s. 207 och 220.

- en myndighet som har rätt att besluta om frihetsberövande åtgärd enligt lagarna om överlämnande eller utlämning för brott (del av 10 § första stycket 8),
- Kriminalvården, när uppgifter behövs för prövning av en fråga enligt fängelselagen (2010:610), lagen (1994:451) om intensivövervakning med elektronisk kontroll, lagen (1991:2041) om särskild personutredning i brottmål m.m., lagen (2015:96) om erkännande och verkställighet av frihetsberövande påföljder inom Europeiska unionen eller lagen (2015:650) om erkännande och verkställighet av frivårdspåföljder inom Europeiska unionen (delar av 10 § första stycket 10),¹¹
- en övervakningsnämnd eller Kriminalvården, i ärenden om övervakning (10 § första stycket 11),¹²
- allmän domstol, i ärenden om omvandling enligt lagen (2006:45) om omvandling av fängelse på livstid (10 § första stycket 16),¹³
- Kronofogdemyndigheten, i ärenden enligt 3 kap. lagen (2009:1427) om erkännande och verkställighet av bötesstraff inom Europeiska unionen och 3 kap. lagen (2011:423) om erkännande och verkställighet av beslut om förverkande inom Europeiska unionen (10 § första stycket 19),¹⁴
- en migrationsdomstol eller Migrationsöverdomstolen, i mål om upphävande av allmän domstols beslut om utvisning på grund av brott, i fråga om den som ärendet gäller (10 § första stycket 20),¹⁵
- en åklagarmyndighet i ärenden enligt förordningen (2014:1553) om förebyggande och lösning av tvister om utövande av jurisdiktion i straffrättsliga förfaranden inom Europeiska unionen (10 § första stycket 22).

¹¹ SOU 2017:29 s. 214, 217–219, 221 f.

¹² A. a. s. 222.

¹³ A. a. s. 225.

¹⁴ I SOU 2017:29 behandlas frågan om hur man ska se på personuppgiftsbehandling vid verkställighet av böter, s. 222 f. Övervägandena gäller dock svenska bötesstraff. Utredningen menar att Kronofogdemyndighetens indrivningsverksamhet inte ska ses som verkställighet av en påföljd, eftersom det inte görs någon skillnad när det gäller indrivning av böter eller andra statliga fordringar. När det gäller utländska bötesdomar handlar det dock inte enbart om indrivning, utan också om utfärdande av s.k. verkställighetsförklaring. Vi menar att detta bör innebära att direktivet är tillämpligt. Jfr även prop. 2012/13:73 s. 61.

¹⁵ SOU 2017:74 s. 517 f.

I några fall som räknas upp i 10 § i förordningen får en bedömning göras från fall till fall. Tillgång till belastningsregistret för chefen för Justitiedepartementet, om utdraget behövs för att fullgöra en skyldighet Sverige har enligt en överenskommelse med en främmande stat (10 § första stycket 2 i förordningen), får bedömas utifrån innehållet i den aktuella överenskommelsen. När det gäller åklagarmyndighetens tillgång i ärenden där en prövning ska göras, beror det också på vad prövningen i det enskilda fallet gäller. Frågor om tillträdesförbud och kontaktförbud faller exempelvis inom det nya dataskyddsdirektivets tillämpningsområde.¹⁶ När det gäller prövningar som Kriminalvården gör enligt häkteslagen (2010:611) beror det nya dataskyddsdirektivets tillämpning på om den person prövningen gäller är frihetsberövad p.g.a. (misstanke om) brott eller av någon annan orsak. Häkteslagen är nämligen tillämplig även på vissa andra frihetsberövanden än anhållande, häktning, verkställighet eller ändring av påföljd.¹⁷

Utlämnande till utländska myndigheter enligt 11, 12 och 14 §§ i lagen samt 24–25 a §§ i förordningen görs, som framgår av bestämmelserna, i huvudsak för brottskampande ändamål (att 11 § i lagen avser sådana ändamål framgår av 24 § i förordningen).¹⁸ Ett undantag torde vara när uppgifter ur det svenska registret behövs i ett utlänningsärende (12 § andra stycket).¹⁹ Vidare framgår av 24 § i förordningen att utlämnanden med stöd av 11 § kan ske för andra ändamål än brottsbekämpning etc. om det finns särskilda skäl. Utlämnanden som inte avser brottmålsförfaranden i enlighet med rambeslutet om kriminalregister (12 a i lagen) torde i de flesta fall omfattas av dataskyddsförordningens tillämpningsområde. På samma sätt som när det gäller svenska myndigheter skulle ett utlämnande utanför ett brottmålsförfarande dock kunna ha syften som omfattas av det nya dataskyddsdirektivet, exempelvis för avgörande av frågor om straffverkställighet.

¹⁶ SOU 2017:29 s. 212 och 228 f.

¹⁷ A. a. s. 192 f.

¹⁸ Att överföra belastningsuppgifter till ett annat land för att dessa ska ingå i ett utländskt kriminalregister (24 c och 25 §§ i förordningen) anser vi omfattas av direktivets tillämpningsområde i enlighet med vår bedömning att förandet av belastningsregistret gör det – förandet av motsvarande register i ett annat land får anses ha samma syften som förandet av det svenska belastningsregistret.

¹⁹ Jfr SOU 2017:29 s. 198 om utlänningskontroll.

Utlämnande enligt 24 b § i förordningen rör inte brottsbekämpning, utan tillstånd och lämplighetsfrågor rörande den som ska bedriva yrkesmässig trafik. Bestämmelsen i 24 a § genomför en bestämmelse om tillgång till belastningsregister i enlighet med det s.k. rörlighetsdirektivet.²⁰ Tillgången till kriminalregister i enlighet med rörlighetsdirektivet avser prövningar som ska göras av EES-medborgares uppehållsrätt i vissa fall då en person kan utgöra ett hot mot allmän ordning och säkerhet. För att en person ska anses utgöra ett sådant hot måste det enligt rörlighetsdirektivet röra sig om konkreta omständigheter som leder till en sådan bedömning (artikel 27 i rörlighetsdirektivet). Sådana prövningar är alltså inte ett led i en regelrätt kontrollverksamhet. Åtgärden innebär inte heller enbart en övervakning utan kan leda till att en EES-medborgare avvisas eller utvisas. Vi menar att det därför ligger närmast till hands att bedöma sådana prövningar som upprätthållande av allmän ordning och säkerhet. Ett utlämnande ur det svenska belastningsregistret för en sådan prövning bör därför omfattas av det nya dataskyddsdirektivets tillämpningsområde.²¹

Utlämnande till andra enskilda än den som begär ett utdrag om sig själv (10 § i lagen och 21 § i förordningen) omfattas av dataskyddsförordningens tillämpningsområde. Visserligen framgår av bestämmelsen i lagen att utlämnande kan ske i fall som har *betydelse för* förebyggande eller beivrande av brott. Med utgångspunkt i den tolkning av det nya dataskyddsdirektivet som Utredningen om 2016 års dataskyddsdirektiv gör kan dock inte sådana utlämnanden, som avser att ge information i anledning av anställning och andra uppdrag hos vissa företag (se 21 § i förordningen) anses ingå i direktivets tillämpningsområde.

²⁰ Europaparlamentets och rådets direktiv 2004/38/EG av den 29 april 2004 om unionsmedborgares och deras familjemedlemmars rätt att fritt röra sig och uppehålla sig inom medlemsstaternas territorier och om ändring av förordning (EEG) nr 1612/68 och om upphävande av direktiven 64/221/EEG, 68/360/EEG, 72/194/EEG, 73/148/EEG, 75/34/EEG, 75/35/EEG, 90/364/EEG, 90/365/EEG och 93/96/EEG. Om genomförandet i svensk rätt, se prop. 2005/06:77 och prop. 2013/14:81.

²¹ Utredningen om 2016 års dataskyddsdirektiv tar inte upp prövningar enligt rörlighetsdirektivet. För svenskt vidkommande är det i första hand Migrationsverket som kan komma att pröva frågor om EES-medborgares uppehållsrätt i vissa fall som bl.a. rör allmän ordning och säkerhet, se 8 kap. 11–14 §§ och 18 § utlänningslagen (2005:716).

Särskilt om utbyte av uppgifter ur medlemsstaternas kriminalregister

Som redogjorts för i avsnitt 5.1 utbyts uppgifter ur nationella kriminalregister inom EU i enlighet med rambeslutet om kriminalregister. I förhållande till det nya dataskyddsdirektivet är rambeslutet en sådan rättsakt som inte påverkas av direktivets ikraftträdande i enlighet med artikel 60.²² Uppgifter utbyts med stöd av rambeslutet inte enbart för syften som omfattas av direktivets tillämpningsområde, utan även för tillstånds- och lämplighetsfrågor m.m. (12 a § i lagen och 41 § i förordningen). Därmed kommer visst uppgiftsutbyte att omfattas av dataskyddsförordningens tillämpningsområde.

5.3 Överväganden om befintliga bestämmelser i förhållande till det nya dataskyddsdirektivet

Bedömning: Bestämmelserna i 1, 2–7, 9, 11–18 och 21 §§ i lagen om belastningsregister och 1–10, 19, 22–24 a och 24 c–41 §§ i förordningen om belastningsregister är bestämmelser som helt eller delvis får betydelse för personuppgiftsbehandling inom det nya dataskyddsdirektivets tillämpningsområde. Bestämmelserna behöver inte ändras som en följd av att dataskyddsdirektivet ska genomföras i svensk rätt. Bestämmelserna i 1 a, 1 b och 20 §§ behöver upphävas eller ändras som en följd av att personuppgiftslagen och lagen (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen kommer att upphävas.

Skälen för bedömningen:

Inledning

I detta avsnitt görs en genomgång av de bestämmelser i lagen och förordningen om belastningsregister som reglerar personuppgiftsbehandling inom det nya dataskyddsdirektivets tillämp-

²² SOU 2017:29 s. 156.

ningsområde. Som framgår anser vi att de flesta bestämmelser kan behållas oförändrade och vi redovisar här skälen för denna bedömning. I de fall vi identifierat behov av förändringar anges skälen även för detta. Våra förslag till förändringar och skälen till att vi utformar dem på ett visst sätt framgår sedan av avsnitt 5.5.

Utgångspunkten för våra överväganden är alltså, som vi redogjort för ovan, att den automatiserade personuppgiftsbehandlingen som förändret av registret innebär, omfattas av det nya dataskyddsdirektivet. För att dataskyddsdirektivet ska bli korrekt genomfört avseende behandlingen i belastningsregistret måste därmed brottsdatalagen tillämpas, eftersom lagen om belastningsregister i sig inte reglerar alla de områden som ingår i direktivet. I våra överväganden nedan utgår vi alltså ifrån att brottsdatalagen är tillämplig på personuppgiftsbehandling som regleras av lagen och förordningen om belastningsregister. Våra förslag till hur detta förhållande ska författningsregleras och vilka följdändringar det för med sig följer i avsnitt 5.5. När vi analyserar bestämmelserna i lagen och förordningen om belastningsregister utgår vi dock i första hand från direktivets reglering, eftersom vi uppfattat vårt uppdrag så att vi ska göra en självständig analys av de ingående författningarnas förhållande till EU-rättsakterna. Samtidigt ska vi givetvis förhålla oss till andra utredningars författningsförslag som får betydelse för tillämpningen av de författningar som ingår i vårt uppdrag.

Skyldigheten att föra registret, personuppgiftsansvar, registrets ändamål och innehåll

Att Polismyndigheten åläggs att föra ett belastningsregister innebär att myndigheten uttryckligen getts en uppgift som omfattas av de syften som ingår i direktivets tillämpningsområde. Bestämmelsen i 1 § är alltså förenlig med dataskyddsdirektivet och genomför kravet på att behandlingen ska ha en rättslig grund (artikel 8).

Att Polismyndigheten pekats ut som personuppgiftsansvarig i 1 § är också förenligt med direktivet (se vidare avsnitt 2.6.3). Att det finns en bestämmelse som reglerar att det är Polismyndigheten som prövar frågor om utlämnande (15 §) får ses som en precisering av vad som ingår i uppgiften att föra registret och i person-

uppgiftsansvaret. Bestämmelserna behöver alltså inte ändras p.g.a. direktivet.

Av artikel 8 i direktivet framgår att ändamål med behandlingen och vilka personuppgifter som får behandlas ska regleras i nationell rätt. Bestämmelserna i 2–5 §§ i lagen, som rör registrets ändamål och innehåll, är alltså även de förenliga med direktivet. Detsamma gäller 2–9 §§ i förordningen som avser registrets innehåll. Bestämmelsen i 1 § i förordningen är endast av upplysande karaktär och påverkas därmed inte av direktivet. I 26–35 §§ i förordningen specificeras vilka myndigheter som ska lämna uppgifter till Polismyndigheten för införande i registret. Myndigheterna i fråga har uppdrag att lagföra brott och verkställa straffrättsliga påföljder. Uppgiftsskyldigheten innebär indirekt en reglering av belastningsregistrets innehåll och är förenlig med dataskyddsdirektivet.

Det kan anmärkas att bestämmelsen i 4 a § i lagen genomför delar av det tidigare nämnda rambeslutet om kriminalregister och bestämmelsen påverkas därmed i och för sig inte av det nya dataskyddsdirektivet i enlighet med artikel 60 (se vidare avsnitt 2.6.3). Samtidigt kan man konstatera att införandet av personuppgifter i belastningsregistret som bygger på utbytet enligt rambeslutet har en rättslig grund i unionsrätten, vilket givetvis också är förenligt med kraven i artikel 8.

Belastningsuppgifter som är känsliga personuppgifter

Belastningsregistret kan innehålla personuppgifter som är sådana särskilda kategorier av personuppgifter som regleras i artikel 10 i direktivet. I svensk rätt kommer sådana särskilda kategorier att kallas *känsliga personuppgifter*, se vidare avsnitt 2.6.4. Exempelvis kan en uppgift om påföljd avslöja förhållanden som rör en dömd persons psykiska hälsa. Att vissa känsliga personuppgifter kan komma att behandlas i belastningsregistret får anses förenligt med artikel 10 i det nya dataskyddsdirektivet. Kraven enligt artikel 10 är att sådan behandling ska följa av nationell rätt, vara absolut nödvändig och att det ska finnas lämpliga skyddsåtgärder. Samtliga dessa krav får anses uppfyllda. Den utförliga författningsregleringen av belastningsregistret får anses i sig utgöra en skyddsåtgärd, liksom tillämpliga sekretessbestämmelser. Det är

absolut nödvändigt att behandla fullständiga uppgifter om alla dömda personer för att belastningsregistret ska fylla sitt syfte.

Direktivets artikel 10 har genomförts i 2 kap. 11 § brottsdatalagen. Förutsättningarna för att behandla känsliga personuppgifter skiljer sig något från direktivets utformning, men behandlingen i belastningsregistret av sådana uppgifter får anses vara förenlig även med bestämmelsen i brottsdatalagen. Vi återkommer i avsnitt 5.5 med förslag i anledning av den sök-begränsning för känsliga personuppgifter som föreskrivs i brottsdatalagen (2 kap.14 §).

Förhållandet till annan reglering av personuppgiftsbehandling

I 1 a och b §§ regleras för närvarande förhållandet till personuppgiftslagen och lagen (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen. Eftersom båda dessa lagar kommer att upphävas måste bestämmelserna upphävas eller innehållet ändras (se vidare avsnitt 2.6.5). Vi återkommer med våra förslag till ändringar i avsnitt 5.5.

Bestämmelser om utlämnande ur registret till svenska myndigheter

I 6 § lagen om belastningsregister finns de grundläggande bestämmelserna om svenska myndigheters möjligheter att få tillgång till uppgifter i belastningsregistret. Som redan redogjorts för kommer inte alla utlämnanden ur registret att omfattas av det nya dataskyddsdirektivets tillämpningsområde, se ovan, avsnitt 5.2 I förordningen om belastningsregister, 10–20 §§, specificeras ytterligare möjligheten att få ut uppgifter. Det är endast vissa utlämnande i 10 §, samt regleringen av direktåtkomst i 19 § som avser brottsbekämpande ändamål.

Att specificera vilka uppgifter som får lämnas ut och i vilka fall får anses förenligt med det nya dataskyddsdirektivet. Den särskilda regleringen av direktåtkomst i 19 § är också förenlig med direktivet, se vidare våra allmänna överväganden, avsnitt 2.6.3.

Den reglering som avser utlämnanden ur registret för andra syften än brottsbekämpning etc. tar vi upp i nästa avsnitt (avsnitt 5.4). Att

uppgifter som först behandlats inom det nya dataskyddsdirektivets tillämpningsområde senare behandlas för andra syften är förenligt med dataskyddsdirektivet om sådan vidarebehandling är reglerad i nationell rätt eller unionsrätten (artikel 9). Författningsregleringen av sådant utlämnande genomför alltså även direktivets krav.

Polismyndighetens utlämnande av uppgifter ur registret till andra svenska myndigheter, både brottsbekämpande sådana och andra, är reglerad som en uppgiftsskyldighet (uppgifterna ska lämnas ut om de begärs, 6 §). Redan av denna anledning blir det inte aktuellt att göra någon prövning enligt 2 kap. 4 § (eller 2 kap. 22 §) brottsdatalagen²³.

Särskilt om Polismyndighetens användning av uppgifter i registret för myndighetens egen brottsbekämpande verksamhet

Att Polismyndigheten kan använda belastningsregistret för brottsbekämpande syften regleras inte på annat sätt i lagen om belastningsregister än genom att denna användning omfattas av registrets ändamål i 2 §.

Enligt det nya dataskyddsdirektivets artikel 4.2 ställs vissa krav på vidarebehandling av personuppgifter inom direktivets tillämpningsområde. Om personuppgifter ska behandlas för ett annat ändamål än det för vilket de samlades in ska dels den personuppgiftsansvarige vara bemyndigad att utföra en sådan behandling, dels ska behandlingen vara nödvändig och proportionerlig till detta andra ändamål. Artikel 4.2 i denna del genomförs i 2 kap. 4 § brottsdatalagen.²⁴ En fråga är på vilket sätt direktivets och brottsdatalagens bestämmelser om ändamål och behandling för nya ändamål ska tillämpas när Polismyndigheten använder uppgifter ur belastningsregistret. Om det är fråga om en behandling för ett *nytt* ändamål gäller kraven på nödvändighet och proportionalitet.

När uppgifter tas in i belastningsregistret sker detta för flera ändamål i enlighet med 2 § lagen om belastningsregister. Ändamålen är av nödvändighet ganska vidsträckta. Användning av uppgifter i registret, däremot, torde (normalt sett) göras för endast ett specifikt ändamål som därtill i de flesta fall kan inordnas under

²³ Bestämmelserna framgår av förslag till ändringar i brottsdatalagen, SOU 2017:74 s. 189 f.

²⁴ SOU 2017:29 s. 684.

endast något av de mer allmänt hållna ändamålen i 2 §. Frågan är då om användning av uppgifter i registret ska anses ske för ett nytt ändamål i enlighet med direktivet och 2 kap. 4 § brottsdatalagen. Vi menar att så inte bör vara fallet. Utredningen om 2016 års data-skyddsdirektiv har gjort bedömningen att insamling av personuppgifter kan ske för flera parallella ändamål.²⁵ Av detta följer, menar vi, att en senare behandling för något av de ursprungliga ändamålen inte kan betraktas som en behandling för ett nytt ändamål. Detta resonemang borde gälla även om ändamålet vid den senare behandlingen har blivit mer preciserat än tidigare. Om Polismyndighetens behandling för brottsbekämpande ändamål inte görs för ett nytt ändamål ställer direktivet inga krav på nödvändighet och proportionalitet i enlighet med artikel 4.2 och någon prövning enligt 2 kap. 4 § brottsdatalagen behöver inte göras. (Däremot gäller givetvis andra krav på behandlingen såsom att den ska ha ett berättigat ändamål, att personuppgifterna ska vara adekvata och relevanta i förhållande till ändamålet, se artikel 4.1 och 2 kap. 3 och 8 §§ brottsdatalagen).

Det kan anmärkas att lagen och förordningen om belastningsregister enbart reglerar förande och behandling av uppgifterna i belastningsregistret, i förekommande fall utlämnanden av sådana uppgifter. När uppgifter om en person lämnat registret och vidarebehandlas för exempelvis en brottsutredning, eller för något annat brottsbekämpande ändamål, blir andra regelverk tillämpliga beroende på vilken verksamhet den fortsatta behandlingen sker i.

Intresseavvägning före utlämnande

I 7 § finns en bestämmelse som berör svenska myndigheter som har möjlighet att få uppgifter ur registret. Bestämmelsen innebär att en myndighet alltid ska göra en intresseavvägning mellan skälet för begäran å ena sidan och den olägenhet eller det men en begäran innebär för den enskilde å den andra. Bestämmelsen är i och för sig tillämplig även om den begärande myndigheten inte utför en automatiserad personuppgiftsbehandling för att få tillgång till uppgifter i belastningsregistret. I praktiken har dock de brotts-

²⁵ A. a. s. 243.

bekämpande myndigheterna direktåtkomst till registret och kommer alltså att utföra en självständig automatiserad personuppgiftsbehandling för att få tillgång till belastningsuppgifter. För behandlingen gäller därmed kravet i brottsdatalagen på att personuppgifter som behandlas ska vara adekvata och relevanta i förhållande till det ändamål för vilket de behandlas (2 kap. 8 §). Intresseavvägningen enligt 7 § ställer dock ett särskilt krav på en myndighet som har möjlighet att få uppgifter ur registret. Det finns inget i direktivet som hindrar en sådan reglering, så länge den inte kan uppfattas som stridande mot direktivets principer för personuppgiftsbehandling. Vi anser att bestämmelsen inte kan uppfattas på det sättet. Snarare får den uppfattas som ett ytterligare skydd för den enskilde än direktivets krav på adekvans etc.²⁶ Starkare skyddsåtgärder för den enskildes rättigheter och friheter är tillåtna enligt direktivets artikel 1.3. Bestämmelsen behöver alltså inte ändras p.g.a. direktivet.

Som vi tidigare redogjort för kommer 2 kap. 4 § brottsdatalagen inte att bli tillämplig på utlämnande ur registret till andra myndigheter, eftersom skyldighet att lämna uppgifterna följer av lagen om belastningsregister. Den proportionalitetsbedömning som ska göras enligt den bestämmelsen kommer alltså inte att bli tillämplig på sådana utlämnanden och kan därmed inte ersätta proportionalitetsbedömningen enligt 7 § lagen om belastningsregister.

Bestämmelser om utlämnande till den registrerade

På begäran kan en enskild få ett utdrag avseende sig själv ur belastningsregistret (9 §). Avgiftsfritt kan ett sådant utdrag lämnas en gång per år. En enskild har också möjlighet att få ett begränsat utdrag om sig själv för vissa angivna syften (9 § andra stycket). Vad de olika begränsade utdragen ska innehålla preciseras i förordningen (22 och 22 a §§). En begäran om utdrag ska vara skriftlig och undertecknad av den sökande (9 § tredje stycket). Det kan nämnas att 22 b och c §§ i förordningen genomför det tidigare nämnda rambeslutet om kriminalregister avseende uppgifter som

²⁶ Jfr Registerutredningens resonemang i SOU 1997:65 s. 152 f.

ska lämnas ut till den enskilde själv om han eller hon är eller har varit medborgare i en annan av EU:s medlemsstater. Dessa bestämmelser berörs alltså inte av det nya dataskyddsdirektivet, enligt vad vi tidigare redogjort för (avsnitt 5.2).

I artikel 14 i det nya dataskyddsdirektivet regleras den registrerades rättigheter när det gäller tillgång till personuppgifter och information om behandlingen. Artikeln genomförs i 4 kap. 3 § brottsdatalagen. Utöver uppgifter om vilka personuppgifter som behandlas, ska den enskilde få skriftlig information om varifrån uppgifterna kommer, den rättsliga grunden för behandlingen, ändamålet med behandlingen, mottagare av personuppgifterna, tid för lagring av dem, rätt att begära rättelse m.m. och uppgifter om möjligheten att lämna in klagomål.

Möjligheten för den enskilde att begära ett utdrag om sig själv enligt 9 § lagen om belastningsregister genomförs alltså till viss del direktivets informationskrav, eftersom det ger den registrerade tillgång till vilka uppgifter om honom eller henne som behandlas i registret. Att den enskilde har möjlighet att i vissa fall begära ut mer begränsade utdrag bör ses som ett utökat skydd, eftersom den registrerade kan ha ett intresse av att kunna visa upp ett utdrag ur belastningsregistret som inte innehåller mer information än vad som är absolut nödvändigt. Att den enskilde har sådana möjligheter är förenligt med direktivet eftersom direktivet medger att medlemsstaterna föreskriver om starkare skydd för enskilda (artikel 1.3).

Utredningen om 2016 års dataskyddsdirektiv har anfört att regleringen av information till den enskilde i enlighet med lagen om belastningsregister är en uttömmande särreglering av informations-skyldigheten vilken gäller före den generella rätten till registerutdrag i brottsdatalagen.²⁷ Om den enskilde begär information enligt brottsdatalagen skulle han eller hon alltså inte få någon information om behandlingen i belastningsregistret, utan vara hänvisad till att begära ett separat registerutdrag enligt lagen om belastningsregister. Frågan är om detta är förenligt med direktivet. Som beskrivits ovan uppfyller utdraget enligt 9 § lagen om belastningsregister inte i alla delar direktivets krav på information när ett registerutdrag lämnas. Om den enskilde inte får den

²⁷ SOU 2017:29 s. 384.

ytterligare information som ska lämnas enligt artikel 14 när han eller hon erhåller ett registerutdrag enligt 9 § är det fråga om en inskränkning av den enskildes rättigheter. Frågan är då om en sådan inskränkning är förenlig med direktivet.

Förutsättningarna för inskränkningar följer av artikel 15.1. Inskränkningar får endast göras för att tillgodose vissa särskilda syften som räknas upp i artikeln, punkterna a–e.

För att avgöra om en inskränkning är möjlig bör man först göra klart för sig vad det är för slags information som ska lämnas enligt artikel 14 i förhållande till personuppgiftsbehandlingen i belastningsregistret. Frågan om inskränkningar handlar ju om vilket motstående intresse, exempelvis att skydda en brottstutredning, som kan påverkas av informationslämnandet.

Kravet på information i artikel 14 avser i stort sett sådant som kan utläsas redan av lagen och förordningen om belastningsregister och brottsdatalagen i sig – det gäller ändamålet med behandlingen, den period under vilken personuppgifterna får behandlas (eller kriterier för hur tidsperioden fastställs), vilka personuppgifter som behandlas och varifrån de kommer, rätten att begära rättelse m.m., och rätten att lämna in klagomål. Det går därmed knappast att hitta några bärande skäl att begränsa sådan information till den registrerade med utgångspunkt från de syften som begränsningar måste ha enligt artikel 15. Sådan information torde kunna utformas tämligen standardiserat.

När det gäller information om *mottagare* är frågan hur specifika krav som direktivet egentligen ställer på denna information. Just att ge väldigt exakt information om vilka mottagare som faktiskt fått ett utdrag ur belastningsregistret skulle kunna skapa svårigheter för Polismyndigheten. Enskilda sökningar loggas visserligen, men av logguppgifterna framgår det inte alltid vem som är mottagare av uppgifterna, endast att en sökning gjorts av en tjänsteman på Polismyndigheten.²⁸ Om polisen skulle behöva ta fram exakt information om mottagare och bevara sådan information för att kunna bifoga den i registerutdrag skulle detta innebära en administrativ börda för myndigheten. Detta är dock i sig inget relevant skäl, utifrån det nya dataskyddsdirektivet, att inskränka den enskildes rätt till information.

²⁸ SOU 2017:29 s. 308.

Utredningen om 2016 års direktiv har dock tolkat rätten till information om mottagare som att den i princip överensstämmer med vad som gäller enligt personuppgiftslagen och 1995 års dataskyddsdirektiv. Information om mottagare kan alltså, enligt utredningen, hållas tämligen allmän.²⁹ Även när det gäller information om mottagare bör därför Polismyndigheten kunna ge ut en standardiserad information om de mottagare eller kategorier av mottagare som följer av lagen och/eller förordningen om belastningsregister i sig. Om man tolkar informationskravet på det sättet framgår det också tydligt att det inte finns några bärande skäl, enligt artikel 15.1 a–e, att inskränka rätten till information.

Slutsatsen av det ovan anförda är alltså att skyldigheten att ge den registrerade tillgång till personuppgifter och information om behandlingen av dem även gäller för den behandling som sker i belastningsregistret. Vi delar den bedömning som Utredningen om 2016 års dataskyddsdirektiv gjort avseende förhållandet mellan informationskravet i brottsdatalagen och rätten till registerutdrag enligt lagen om belastningsregister, som alltså innebär att lagen om belastningsregister kommer att gälla istället för brottsdatalagen om den nuvarande utformningen av lagens bestämmelse om registerutdrag behålls. För att genomföra direktivet krävs alltså någon form av ändring i lagen om belastningsregister. Vi överväger olika alternativ i avsnitt 5.5.

Bestämmelser om utlämnande till utländska myndigheter

Utlämnande ur belastningsregistret till utländska myndigheter i brottsbekämpande syften regleras i huvudsak i 11, 12 och 14 §§ i lagen och i bestämmelserna i 24, 24 a och 24 c – 25 a §§ i förordningen. Även utlämnanden enligt 12 a § kan vara för syften som omfattas av det nya dataskyddsdirektivet (se en närmare redogörelse i avsnitt 5.2). Som redan anförts ovan förhindrar inte det nya dataskyddsdirektivet en närmare nationell reglering av utlämnande. Detta ställningstagande förändras inte av att regleringen gäller utländska myndigheter. Flera av bestämmelserna i förordningen rör uppgiftsutbytet enligt det tidigare nämnda

²⁹ A. a. s. 380.

rambeslutet om kriminalregister. Sådan reglering påverkas inte av det nya dataskyddsdirektivet, i enlighet med vad som anförts tidigare (avsnitt 5.2).

När det gäller gränsöverskridande utbyte av personuppgifter som innebär en automatiserad behandling finns en särskild reglering av överföring till tredje land och internationella organisationer i det nya dataskyddsdirektivet. Direktivet genomförs i detta avseende i 8 kap. brottsdatalagen. Bestämmelserna om utlämnande i lagen och förordningen om belastningsregister möjliggör ett uppgiftsutlämnande till tredje land genom att uppgiftsutbyte tillåts ske med Interpol och länder anslutna till Interpol. Om personuppgifterna behandlas helt eller delvis automatiserat för att överföras till tredje land måste de förutsättningar som följer av 8 kap. brottsdatalagen också vara uppfyllda för att överföringen ska kunna ske. Regleringen av tredjelandsöverföringar i 33–35 §§ personuppgiftslagen ersätts alltså, såvitt avser överföring för de syften som omfattas av direktivet, av 8 kap. brottsdatalagen.³⁰

Gallring

Som anförts i våra generella överväganden (avsnitt 2.6.3) hindrar inte det nya dataskyddsdirektivet att tidsfrister för bevarande regleras i författning. Enligt direktivet är det t.o.m. en skyldighet för medlemsstaterna att bestämma närmare tidsfrister för radering och lagring (artikel 5). De bestämmelser som rör gallring i lagen om belastningsregister kan alltså i och för sig behållas (16–18 §§). Bestämmelsen i 17 a § genomför delar av rambeslutet om kriminalregister och påverkas därmed inte heller av det nya dataskyddsdirektivet, som redan redogjorts för (se avsnitt 5.2).

I nästa avsnitt överväger vi om det annars finns skäl att förändra ordalydelsen av de nuvarande gallringsbestämmelserna med hänsyn till de förslag som Utredningen om 2016 års dataskyddsdirektiv lämnar om gallring och längsta tid för behandling av personuppgifter.

³⁰ Jfr prop. 2009/10:85 s. 203, jfr s. 321 och s. 330.

Rättelse och skadestånd

Bestämmelsen i 20 § hänvisar till personuppgiftslagen och måste därför anpassas till att denna lag upphör och att brottsdatalagen i stället ska tillämpas. Vi lämnar förslag i avsnitt 5.5.

Användningsbegränsningar

När medlemsstaterna efter begäran utbyter uppgifter ur sina kriminalregister i enlighet med rambeslutet om kriminalregister har de rätt att ställa upp användningsbegränsningar. Uppgifterna får heller inte användas för andra ändamål än dem de begärdes för. Att svenska myndigheter har en skyldighet att respektera användningsbegränsningar i enlighet med rambeslutet följer av 21 § i lagen om belastningsregister. I 24 e och f §§ i förordningen om belastningsregister finns vissa ytterligare bestämmelser om användningsbegränsningar som Polismyndigheten kan ställa upp vid utlämnande enligt rambeslutet.

Eftersom det nya dataskyddsdirektivet inte är avsett att påverka tidigare EU-rättsakter om informationsutbyte på området för polis- och straffrättsligt samarbete påverkas inte de nämnda bestämmelserna av direktivets reglering i enlighet med artikel 60.³¹ Det framgår av bestämmelsen i 21 § att den gäller oavsett vad som föreskrivs i annan författning. Den kommer därmed att gälla i stället för 2 kap. 20 § brottsdatalagen, som annars innebär att användningsbegränsningar i förhållande till andra medlemsstater inte får ställas upp om det inte finns någon sådan möjlighet i förhållande till svenska mottagare.

Avgifter för utdrag ur registret

Enligt 23 § i förordningen får avgift tas ut för utdrag ur registret, dels för vissa sådana begränsade utdrag som tidigare beskrivits och som kan lämnas till den registrerade själv, dels för utdrag till andra enskilda. Det nya dataskyddsdirektivet innebär att information enligt direktivet som en utgångspunkt ska vara avgiftsfri

³¹ Se även SOU 2017:29 s. 290 f.

(artikel 12.4) vilket genomförs i 4 kap. 12 § brottsdatalagen. Den information som avgiftsbeläggs i förordningen om belastningsregister avser dock information som går utöver vad som regleras i direktivet, enligt vad som tidigare anförts i detta avsnitt. Bestämmelserna i 23 § påverkas därmed inte av direktivet.

Ansvar för lämnade uppgifter

I 36–37 §§ i förordningen finns bestämmelser om ansvar för inlämnade uppgifters riktighet och rättelse av felaktiga uppgifter. Bestämmelserna avser felaktigheter som upptäcks av de inblandade myndigheterna och alltså inte den enskildes rätt till rättelse. Såvitt avser behöriga myndigheter, vars uppgiftslämnande omfattas av direktivets tillämpningsområde, kan bestämmelserna ses som preciseringar av principen om att personuppgifter ska vara korrekta (artikel 4.1 d som genomförs i 2 kap. 7 § brottsdatalagen). Förordningens bestämmelser kan därmed anses genomföra direktivet i denna del och utgör en precisering i förhållande till bestämmelsen i brottsdatalagen. De kan och bör därför behållas i förordningen.

Föreskriftsrätt

I 5 och 13 §§ i lagen och 38 och 39 §§ i förordningen finns bestämmelser om föreskriftsrätt. Bestämmelserna påverkas inte av det nya direktivet, se vidare våra allmänna överväganden, avsnitt 2.6.3.

Skyldighet att inhämta uppgifter ur registret

Domstolar har en skyldighet att inhämta ett utdrag ur belastningsregistret innan någon döms till vissa uppräknade påföljder (40 § i förordningen). Personuppgiftsbehandlingen för sådana inhämtanden sker i syfte att lagföra brott, och faller alltså under det nya dataskyddsdirektivets tillämpningsområde. Åliggandet är en precisering av i vilka situationer och för vilka ändamål uppgifter inhämtas ur belastningsregistret och får därmed anses förenligt

med direktivet. Syftet är ju för övrigt att tillförsäkra den som är tilltalad i brottmål en lagenlig bedömning i påföljdsfrågan.

Möjlighet att inhämta uppgifter med stöd av rambeslutet

1 41 § regleras myndigheters möjligheter att via Polismyndigheten begära uppgifter ur andra medlemsstaters kriminalregister med stöd av rambeslutet om kriminalregister. Som tidigare redogjorts för påverkar inte det nya dataskyddsdirektivet det uppgiftsutbyte som sker i enlighet med rambeslutet om kriminalregister. Samtidigt kan det konstateras att det inte strider mot direktivet att författningsreglera informationsutbyte inom direktivets tillämpningsområde.

5.4 Överväganden om befintliga bestämmelser i förhållande till dataskyddsförordningen

Bedömning: Bestämmelserna i 6–8, 10, 11, 12 a, 19 och 21 §§ lagen om belastningsregister samt 10–21, 23, 24 b och 41 §§ förordningen om belastningsregister avser, helt eller delvis, behandling av personuppgifter inom dataskyddsförordningens tillämpningsområde. Bestämmelserna är förenliga med förordningen och några författningsändringar behöver inte göras till följd av att förordningen börjar tillämpas.

Skälen för bedömningen:

Inledning

Vi har tidigare konstaterat att förändret av belastningsregistret får anses falla under det nya dataskyddsdirektivets tillämpningsområde. Att dataskyddsförordningen också blir tillämplig på viss behandling i registret beror på att ändamålen med en del uttag ur registret inte avser brottsbekämpning, lagföring eller något annat av de ändamål som avses i artikel 2.2 d i dataskyddsförordningen och artikel 1.1 i det nya dataskyddsdirektivet.

I detta avsnitt bedömer vi de bestämmelser som vi menar reglerar behandling inom dataskyddsförordningens tillämpningsområde. Samma bestämmelser kan vara tillämpliga även på behandling inom det nya dataskyddsdirektivets område, exempelvis 7 §. Följden av att behandlingen i belastningsregistret ibland omfattas av dataskyddsförordningens, ibland det nya dataskyddsdirektivets tillämpningsområde, är alltså att vissa bestämmelser måste bedömas utifrån båda EU-rättsakternas krav.³²

Vi bedömer att det är 6–8, 10, 11, 12 a, 19 och 21 §§ lagen om belastningsregister samt 10–21, 24 b och 41 §§ i förordningen om belastningsregister som innehåller de bestämmelser som ska bedömas med beaktande av dataskyddsförordningen. Som följer av våra överväganden nedan anser vi att bestämmelserna är förenliga med förordningen.

Myndigheters tillgång till uppgifter i belastningsregistret

Att Polismyndigheten gör uttag ur belastningsregistret för att lämna dem till andra myndigheter för prövningar i tillstånds- och lämplighetsfrågor eller använder uppgifterna för myndighetens egna prövningar för sådana ändamål får anses vara behandling för att utföra en uppgift av allmänt intresse (artikel 6.1 e). Utlämnandena är reglerade i författning, liksom de prövningar i sig som uppgifterna ur belastningsregistret behövs för. Kraven på rättslig grund och att denna ska vara fastställd i nationell rätt (artikel 6.1 och 6.3) är alltså uppfyllda.

Att författningsregleringen tydligt preciserar i vilka fall och för vilka ändamål utlämnanden får ske är vidare förenligt med artikel 6.2 och 6.3. Bestämmelserna i 6 § lagen om belastningsregister är därmed förenliga med dataskyddsförordningen, liksom de ytterligare preciseringar av utlämnande som finns i 10–20 §§ i förordningen om belastningsregister. Som vi redan berört reglerar 10 § i förordningens endast delvis utlämnanden för syften som omfattas av dataskyddsförordningens tillämpningsområde. Även när det gäller 19 § i förordningen berörs den endast av dataskydds-

³² Jfr Fi2017/02899/S3 s. 124 f.

förordningen i den mån direktåtkomsten kan utnyttjas för andra ändamål än brottsbekämpning etc.

Även regleringen i 8 § i lagen om belastningsregister som möjliggör utlämnande för statistiska ändamål är, i enlighet med det ovan anförda, förenlig med dataskyddsförordningen. Vi menar att det inte ingår i vårt uppdrag att analysera om de särskilda förutsättningarna i artikel 89 avseende behandling för statistiska ändamål är uppfyllda, eftersom denna behandling i sig inte regleras av lagen om belastningsregister.³³

För den reglering som möjliggör utlämnande till utländska myndigheter för ändamål inom dataskyddsförordningens tillämpningsområde (dvs. 11 och 12 a §§ i lagen samt 24 och 24 b §§ i förordningen), gäller också de ovan gjorda bedömningarna – författningsregleringen kan ses som en rättslig grund för utlämnanden och därtill en tillåten precisering av i vilka situationer behandling är tillåten. De utlämnande som regleras av 12 a § följer av rambeslutet om kriminalregister och personuppgiftsbehandlingen har alltså även en rättslig grund i unionsrätten. Utlämnanden enligt 11 § kan omfattas av dataskyddsförordningens tillämpningsområde (men även av det nya dataskyddsdirektivet, vilket bl.a. framgår av 24 § i förordningen). Man får utgå från att utlämnanden som ligger inom ramen för internationella överenskommelser eller EU-rättsakter har ett allmänintresse som grund eller att personuppgiftsbehandling till följd av överenskommelsen eller EU-rättsakten är en rättslig förpliktelse. Även 11 § är alltså förenlig med dataskyddsförordningen. I förordningen (24 b §) preciseras ett utlämnande enligt 11 § för ändamål inom dataskyddsförordningens tillämpningsområde, nämligen då det gäller prövning av personer som ska bedriva yrkesmässig trafik. Regleringen har i detta fall både en unionsrättslig grund och ett tydligt allmänintresse som gör den förenlig med dataskyddsförordningen.

Om utlämnanden som inte avser brottsbekämpning skulle komma i fråga till ett tredje land ska dataskyddsförordningens särskilda reglering av sådana utlämnanden tillämpas, om utlämnandet innebär en helt eller delvis automatiserad behandling, jfr vad

³³ Det kan dock noteras att behandlingen är författningsreglerad i förordningen (2001:100) om den officiella statistiken och därtill omgärdad av vad som får betraktas som skyddsåtgärder för den enskilde i och med gällande sekretessreglering i 24 kap. 8 § första stycket offentlighets- och sekretesslagen (2009:400).

som sagts ovan om utlämnanden till tredje land inom brottsdatalogens tillämpningsområde.

Slutligen ska anmärkas att dataskyddsförordningens särskilda reglering avseende behandling av lagöverträdelser (artikel 10) inte ställer några krav när det gäller myndigheters behandling av sådana personuppgifter. Vi återkommer nedan till artikelns betydelse för utlämnande till enskilda.

Särskilt om Polismyndighetens egen användning av uppgifter för ändamål utanför brottsdatalogens tillämpningsområde

På samma sätt som när det gäller brottsbekämpande ändamål regleras Polismyndighetens egen användning av belastningsregistret för andra syften än brottsbekämpning inte på annat sätt än genom registrets ändamålsbestämmelser. Eftersom Polismyndighetens användning av uppgifter i registret för ändamål i enlighet med 2 § första stycket 4 i huvudsak torde omfattas av dataskyddsförordningens tillämpningsområde blir 2 kap. 22 § brottsdatalogen och den proportionalitetsprövning som framgår av andra stycket i den paragrafen tillämplig. Detta gäller, som det får förstås, även om behandlingen i och för sig inte görs för ett nytt ändamål i förhållande till det ursprungliga behandlingsändamålet (jfr vad vi framfört i föregående avsnitt om tillämpningen av 2 kap. 4 § brottsdatalogen). Vi diskuterar i nästa avsnitt (avsnitt 5.5) om denna ordning är lämplig eller inte.

Inhämtande av uppgifter i enlighet med rambeslutet om kriminalregister

Möjligheten att hämta in belastningsuppgifter från andra europeiska länder regleras i 41 § förordningen om belastningsregister. En sådan begäran kan alltså gälla för syften både inom och utom det nya dataskyddsdirektivets tillämpningsområde, vilket då i förekommande fall innebär att dataskyddsförordningen blir tillämplig. I den mån uppgiftslämnande innefattar en automatiserad behandling av personuppgifter innebär i sådana fall den nationella regleringen och, inte minst regleringen på EU-nivå, att det finns en rättslig grund för sådan personuppgiftsbehandling.

Vid inhämtande av uppgifter gäller användningsbegränsningen i 21 § i lagen. Att medlemsstaterna ställer upp användningsbegränsningar vid informationsutbyte i enlighet med EU-rättsakter kan inte anses strida mot dataskyddsförordningen, en sådan möjlighet kan snarast ses som en precisering av principen om ändamålsbegränsning i artikel 5.1 b.

Intresseavvägningen enligt 7 §

I 7 § finns, som tidigare beskrivits, en bestämmelse som innebär en skyldighet för en myndighet som begär ut uppgifter ur registret att alltid göra en avvägning mellan behovet av information och den enskildes intresse av att uppgifter *inte* inhämtas. Bestämmelsen riktar sig alltså till samtliga myndigheter som har möjlighet att få uppgifter ur registret, även myndigheter som inte är att anse som behöriga i det nya dataskyddsdirektivets mening. Det ska noteras att bestämmelsen gäller oavsett om en myndighet utför en automatiserad personuppgiftsbehandling för att begära uppgifter och/eller sedan automatiserat behandlar uppgifterna vidare. För en myndighet som behandlar uppgifterna automatiserat skulle man i och för sig kunna diskutera om bestämmelsen, på samma sätt som inom det nya dataskyddsdirektivets tillämpningsområde, utgör en dubbelreglering i förhållande till principen om uppgiftsminimering, som återfinns både i det nya dataskyddsdirektivet och i dataskyddsförordningen (artikel 5.1 c). Som vi anført i avsnitt 5.3 menar vi att 7 § lagen om belastningsregister ger ett starkare skydd än principen om uppgiftsminimering. Det är förenligt med dataskyddsförordningen att lagstiftaren begränsar myndigheters personuppgiftsbehandling ytterligare, utöver de begränsningar som kan följa av förordningen, se våra allmänna överväganden, avsnitt 2.5.3. Bestämmelsen bör därför behållas oförändrad även inom dataskyddsförordningens tillämpningsområde.

Utlämnande till enskilda

Enskilda kan få ta del av uppgifter om andra enskilda i belastningsregistret. Det gäller dels i vissa anställningsärenden, dels om en enskild kan styrka att hans eller hennes rätt är beroende av

uppgifterna i fråga (10 § i lagen). Vilka anställningsärenden det kan vara fråga om preciseras i 21 § i förordningen.

Bestämmelser om utlämnande kan generellt sägas vara en sådan precisering som faller in under artikel 6.2 i dataskyddsförordningen. Behandlingen får anses ha en rättslig grund antingen i 6.1 c eller e i förordningen. Eftersom utlämnandet är lagreglerat och innebär att uppgifter ska lämnas ut under vissa angivna förutsättningar kan man betrakta behandlingen som följande av en rättslig förpliktelse, som i det här fallet alltså gäller för Polismyndigheten som registerförare. Att det finns en möjlighet för enskilda som är ansvariga för viss verksamhet där det är av särskild vikt att bedöma lämpligheten hos den som ska anställas får därtill anses vara av allmänt intresse. Även den generella möjligheten att i vissa andra fall få information om en annan enskild bör kunna betraktas som ett allmänt intresse.

Eftersom bestämmelsen medger att uppgifter lämnas ut till andra än myndigheter måste samtidigt förordningens särskilda reglering av uppgifter om fällande domar i brottmål beaktas (artikel 10). Utlämnandet behöver i och för sig inte innebära att mottagaren har möjlighet att *behandla* uppgifterna i förordningens mening. Uppgifter till enskilda lämnas företrädesvis ut i pappersform. Behandling av uppgifter om fällande domar i brottmål är heller inte helt förbjuden enligt förordningen, om den regleras i nationell rätt som fastställer lämpliga skyddsåtgärder. Den tystnadsplikt som gäller för enskilda enligt 19 § bör bedömas som en sådan skyddsåtgärd. Bestämmelsen är därmed i sig förenlig med förordningen. Tystnadsplikten förhindrar att enskilda använder uppgifterna som erhållits för ytterligare behandling som innebär att uppgifterna sprids. Vidare kan anmärkas att Dataskyddsutredningen har föreslagit att en reglering motsvarande 21 § personuppgiftslagen tas in i 3 kap. 9 § dataskyddslagen. Den nya regleringen kommer, liksom nuvarande bestämmelse i personuppgiftslagen, att innebära ett förbud för andra än myndigheter att behandla personuppgifter som rör fällande domar i brottmål. En automatiserad vidarebehandling av uppgifter som erhållits ur belastningsregistret är därmed inte tillåten enligt dataskyddslagen.

Slutligen ska nämnas att avgift tas ut för utdrag som begärs av enskilda (23 § i förordningen). Bestämmelsen avser inte en reglering av personuppgiftsbehandlingen i sig och påverkas därmed inte av dataskyddsförordningen.

Behandling av personnummer och känsliga personuppgifter

Behandlingar för utlämnande som faller under dataskyddsförordningens tillämpningsområde innebär (liksom givetvis behandlingar som faller under det nya dataskyddsdirektivets) behandling av personnummer. (Personnummer är en grundläggande uppgift om den enskilde i registret enligt 2 § i förordningen om belastningsregister). Som framgår av våra allmänna överväganden finns en bestämmelse i dataskyddsförordningen som särskilt avser nationella identifikationsnummer – artikel 87. Av våra allmänna överväganden framgår också att det i viss mån är tveksamt vilka krav artikel 87 ställer på regleringen av personnummer. För det fall artikelns krav på skyddsåtgärder är tillämpliga på regleringen i belastningsregistret, menar vi att detta krav får anses uppfyllt. Belastningsregistrets författningsreglering och tillämpliga sekretesbestämmelser får anses vara mer än tillräckliga skyddsåtgärder eftersom regleringen tydligt avgränsar användningen av personuppgifter i registret. När uppgifter ur belastningsregistret lämnas ut till en enskild har denne tystnadsplikt, vilket också innebär ett skydd för den registrerade. Vidare är användandet av personnummer i belastningsregistret klart motiverat utifrån behovet av en säker identifiering och överensstämmer därmed med de allmänna krav som ställs enligt 3 kap. 13 § dataskyddslagen. Sammanfattningsvis anser vi alltså att behandlingen av personnummer i belastningsregistret är förenlig med dataskyddsförordningen.

Som vi anförde i avsnitt 5.3 kan behandling av personuppgifter i belastningsregistret innebära en behandling av känsliga personuppgifter. Möjligheten att behandla belastningsuppgifter för syften inom dataskyddsförordningens tillämpningsområde får anses förenlig med regleringen i 3 kap. 3 § 3 dataskyddslagen (dvs. behandlingen är absolut nödvändig för sitt ändamål och innebär inte ett otillbörligt intrång i den registrerades personliga integritet) och därmed med dataskyddsförordningen (jfr våra allmänna överväganden, avsnitt 2.5.6).

5.5 Överväganden om och förslag till författningsändringar

Förslag: I lagen om belastningsregister ges 1 a § ett nytt innehåll som anger att lagen gäller utöver brottsdatalagen. Vidare införs en bestämmelse i paragrafen som innebär att sökbegränsningen i 2 kap. 14 § brottsdatalagen inte hindrar sökningar i belastningsregistret på brottsrubricering och verkställighet av påföljd.

Den nuvarande bestämmelsen i 1 b § upphävs och i stället införs en ny paragraf (en ny 1 b §) som anger att lagens bestämmelser kompletterar dataskyddsförordningens reglering i vissa fall och att dataskyddslagen också gäller för sådan behandling.

Ändamålen med belastningsregistret i 2 § anpassas till brottsdatalagens terminologi såvitt avser de brottsbekämpande myndigheternas användning av uppgifter ur registret.

Möjligheten att begära obegränsade registerutdrag ska inte längre regleras av lagen om belastningsregister utan av brottsdatalagen. Kravet på egenhändigt undertecknande av en begäran om utdrag (9 § fjärde stycket) ersätts med att Polismyndigheten ska säkerställa att begäran har gjorts av en behörig person.

Bestämmelsen i 20 § ändras så att en hänvisning görs till brottsdatalagens bestämmelser om skadestånd. Hänvisningen till personuppgiftslagen tas bort.

Bedömning: Bestämmelserna om gallring bör stå kvar oförändrade. Några bestämmelser som avser inskränkning i den registrerades rättigheter enligt det nya dataskyddsdirektivet eller dataskyddsförordningen behövs inte. Bestämmelser om sanktionsavgifter behövs inte heller.

Skälen för förslaget och bedömningen:

Förhållandet till annan lagstiftning – 1 a och 1 b §§

Som tidigare angetts måste 1 a § ändras eftersom den hänvisar till personuppgiftslagen, som kommer att upphävas som en följd av den nya EU-regleringen. Bestämmelsen i 1 b § hänvisar till en annan författning som kommer att upphävas – lagen (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen. Istället för det nuvarande innehållet i 1 a och 1 b §§ bör införas bestämmelser som klargör förhållandet till den nya generella regleringen av personuppgiftsbehandling – brottsdatalagen, dataskyddsförordningen och dataskyddslagen.³⁴

Liksom andra registerförfattningar som gäller inom det nya dataskyddsdirektivets tillämpningsområde bör det anges att lagen om belastningsregister gäller *utöver* brottsdatalagen, se vidare avsnitt 2.6.7.

När det gäller sökbegränsningen avseende känsliga personuppgifter i 2 kap 14 § brottsdatalagen menar vi att vissa undantag bör göras. Vi menar också att förhållandet mellan informations-skyldigheten enligt 4 kap. 3 § och 9 § lagen om belastningsregister behöver regleras för att förtydliga vad som gäller. Dessa frågor behandlas vidare nedan. Som vi diskuterat ovan (avsnitt 5.3) skulle en viss tveksamhet kunna uppstå om tillämpningen av 2 kap. 4 § brottsdatalagen i förhållande till Polismyndighetens användning av uppgifter ur belastningsregistret för brottsbekämpande ändamål. Vi menar dock att det inte finns behov av att införa någon författningsreglering som avser denna fråga, utan att den kan klargöras tillräckligt i författningskommentaren.

När det gäller dataskyddsförordningen anser vi att det bör anges som en upplysning att lagen kompletterar förordningen (se vidare våra generella överväganden, avsnitt 2.5.9). Man hade i och för sig kunnat helt undvara en hänvisning till dataskyddsförordningen med motiveringen att det framgår av brottsdatalagen i sig att vissa behandlingar av uppgifter, som från början samlats in och behandlats inom tillämpningsområdet för brottsdatalagen, sedermera

³⁴ Upphävande av 1 b § föreslås också av Utredningen om 2016 års dataskyddsdirektiv som en följd av utredningens förslag att 2013 års lag ska upphävas, se SOU 2017:74 s. 72.

kan komma att behandlas för syften som gör dataskyddsförordningen tillämplig i stället (2 kap. 22 §).³⁵ Vi menar dock att det kan vara befogat att ha en sådan bestämmelse även i lagen om belastningsregister, så att det redan av den lagen framgår att behandlingen i registret kan komma att omfattas antingen av brottsdatalagens eller av dataskyddsförordningens tillämpningsområde.

I den upplysande bestämmelsen som tar upp dataskyddsförordningen bör också anges att dataskyddslagen gäller, se vidare våra överväganden om behovet av författningsreglering av förhållandet mellan registerförfattningar och dataskyddslagen, avsnitt 2.5.9.

Undantag från sökbegränsningen för känsliga personuppgifter

Utredningen om 2016 års dataskyddsutredning föreslår för de flesta registerförfattningar som gäller för behöriga myndigheters personuppgiftsbehandling att det ska göras vissa undantag från sökbegränsningen avseende känsliga personuppgifter som följer av 2 kap. 14 § brottsdatalagen.³⁶ Eftersom någon sådan sökbegränsning inte finns i personuppgiftslagen kan sökningar i belastningsregistret i dag göras exempelvis med brottsrubriceringar eller uppgifter om verkställighet av påföljd som sökbegrepp. Det finns behov för de behöriga myndigheterna att kunna göra sådana sökningar och därför uppstår samma behov att göra undantag från brottsdatalagens sökbegränsning i belastningsregistret som i andra informationsinsamlingar hos de brottsbekämpande myndigheterna. Vissa av undantagen som görs i andra registerförfattningar blir dock inte aktuella vid sökningar i belastningsregistret, såsom sökningar avseende personers utseende eller religiösa övertygelse, eftersom sådana uppgifter inte förekommer i belastningsregistret.

³⁵ 2 kap. 21 § enligt förslaget i SOU 2017:29, ändrad till 2 kap. 22 § i SOU 2017:74, se s. 190 f.

³⁶ Se exempelvis förslaget till 2 kap. 5 § polisens brottsdatalog (s. 97 i SOU 2017:74) och överväganden till förslaget (a. a. s. 423–426).

Proportionalitetsprövningen enligt 2 kap. 22 §

Som vi redan nämnt kommer 2 kap. 22 § brottsdatalagen att bli tillämplig på Polismyndighetens egen användning av uppgifter ur belastningsregistret för olika lämplighets- och tillståndsprövningar. (Däremot inte på Polismyndighetens behandling för att lämna ut uppgifter för sådana ändamål till svenska myndigheter, eftersom utlämnandet följer av en uppgiftsskyldighet).

Den prövning som ska göras enligt 2 kap. 22 § andra stycket har föreslagits av Utredningen om 2016 års dataskyddsdirektiv och hänger samman med utredningens förslag om att sekundära ändamål inte längre ska regleras i vissa registerförfattningar inom brottsdatalagens tillämpningsområde. Bestämmelsen ska också ses tillsammans med den reglering som föreslås i 2 kap. 4 § brottsdatalagen, som innebär att en prövning av nödvändighet och proportionalitet ska göras innan personuppgifter behandlas för nya ändamål inom brottsdatalagens tillämpningsområde. Utredningen anför bl.a. att det skulle skapa en omotiverad skillnad att kräva en noggrannare prövning för behandling för nya ändamål inom brottsdatalagens tillämpningsområde än utanför det.³⁷

Belastningsregistrets användning utanför brottsdatalagens tillämpningsområde, menar vi, kan inte sägas innebära en behandling för nya ändamål, eftersom samtliga ändamål för registret som regleras i 2 § gäller redan vid insamlandet av uppgifter till registret. Lagen om belastningsregister innehåller alltså inga sekundära ändamål på samma sätt som många andra registerförfattningar. Frågan är då om det verkligen är motiverat att 2 kap. 22 § ska tillämpas vid Polismyndighetens egen användning av registret för ändamål inom dataskyddsförordningens tillämpningsområde. Vi har gjort bedömningen att 2 kap. 4 § inte blir tillämplig när Polismyndigheten använder registret för brottsbekämpande ändamål. Om 2 kap. 22 § ska tillämpas när Polismyndigheten använder registret för andra ändamål innebär det att högre krav ställs på sådan behandling än på behandling inom brottsdatalagens

³⁷ SOU 2017:74 s. 398 f.

tillämpningsområde. Detta är dock knappast orimligt i och för sig.³⁸

Däremot kan man hävda att tillämpningen av 2 kap. 22 § skapar en omotiverad skillnad mellan Polismyndighetens egen användning av registret och utlämnande till andra myndigheter — eftersom den sistnämnda behandlingen beror på en uppgiftsskyldighet behövs ingen prövning i de fallen. Å andra sidan är de myndigheter som begär uppgifter skyldiga att göra en proportionalitetsprövning enligt 7 § lagen om belastningsregister.

Det bör också poängteras att en tillämpning av 2 kap. 22 § inte kan förutsättas förhindra någon användning av belastningsregistret som i dag är laglig. I de allra flesta fall bör en prövning i enlighet med bestämmelsen utfalla så att uppgifter kan behandlas på samma sätt som i dag, eftersom det får anses både nödvändigt och proportionerligt.

Det finns alltså argument både för och emot att 2 kap. 22 § ska vara tillämplig på Polismyndighetens behandling för ändamål utanför brottsdatalogens tillämpningsområde. Bestämmelsen är inte nödvändig för att genomföra något krav som följer av någon av EU-rättsakterna. Ett undantag skulle därmed kunna göras i lagen om belastningsregister, lämpligen i 1 a §, där ett annat undantag från brottsdatalogen tas in. Vi lämnar dock inget sådant förslag. En sådan reglering är inte nödvändig som en anpassning till EU-rättsakterna i sig och ligger därmed egentligen inte inom vårt uppdrag. Frågan hänger också så nära samman med annan reglering inom brottsdatalogens tillämpningsområde att den lämpligen bör övervägas vidare inom ramen för det lagstiftningsarbetet. Bl.a. bör det ha betydelse hur man ska se på 2 kap. 22 § i relation till andra register som förs av Polismyndigheten, exempelvis dna-registret, som förs för ändamål både inom och utanför brottsdatalogens tillämpningsområde.³⁹

³⁸ Att ställa högre krav för att få vidarebehandla uppgifter utanför brottsdatalogens tillämpningsområde än inom tillämpningsområdet kan istället ses som den rimligaste ordningen, jfr Utredningen om 2016 års dataskyddsdirektiv, a. a. s. 399.

³⁹ Se 5 kap. 1 § polisens brottsdatalog (SOU 2017:74 s. 109). Dna-registret förs för brottsbekämpande syften, men även för att underlätta identifiering av avlidna personer (första stycket 4). Utredningen om 2016 års dataskyddsdirektiv har inte närmare utvecklat hur 2 kap. 22 § ska tillämpas vid användning av dna-registret för detta ändamål.

Justering av ändamålen med belastningsregistret

Vi ger i andra avsnitt i denna promemoria uttryck för att vi tror att det kan underlätta för myndigheter som har att tillämpa flera olika författningar som rör personuppgiftsbehandling att författningarna använder sig av samma reglering och samma uttryckssätt så långt det är möjligt och om det inte finns sakliga skäl emot en sådan ordning. I lagen om belastningsregister tas ändamålen för registret upp i 2 §. Första punkten avser ändamålen att förebygga, upptäcka och utreda *brott*. Brottssdatalagens tillämpningsområde tar istället upp, såvitt nu är relevant, syftena att förebygga, *förhindra* eller upptäcka *brottslig verksamhet* och utreda *brott*. Vi har tidigare anfört att vi menar att det grundläggande ändamålet med belastningsregistret är sådant att det nya dataskyddsdirektivet är tillämpligt på förändret av registret. Det framstår som en mer konsekvent och lättillämpad ordning om ändamålen i lagen om belastningsregister ansluter till brottssdatalagens uttryckssätt.

Även om ändamålen för belastningsregistret är kopplade till begreppet *brott*, som vanligtvis uppfattas som snävare än termen *brottslig verksamhet*, menar vi att någon större saklig skillnad inte kan anses föreligga just i detta fall. Bestämmelserna om ändamål i lagen om belastningsregister utformades i anslutning till tillämpningsområdet för 1998 års polisdatlag⁴⁰, som också använde uttryckssätten *förebygga* och *utreda brott*. Utgångspunkten torde ha varit den ursprungliga lydelsen av 2 § polislagen (1984:387)⁴¹, som också angav förebygga och utreda brott som några av de verksamheter som utgör polisens uppdrag. 1998 års polisdatlag omfattade dock inte endast behandling av uppgifter för utredning av konkreta brottsmisstankar, utan även uppgifter som behövdes för underrättelseverksamhet (vilket framgår bl.a. av 1 § och 3 § i lagen). Såvitt avsåg polisdatatalagen förändrades uttryckssättet genom införandet av 2010 års polisdatlag, bl.a. på så sätt att begreppet *brottslig verksamhet* togs in i ändamålen för behandling. Någon egentlig utvidgning av ändamålen var dock inte avsedd, utan utgångspunkten var alltså polisens uppgifter enligt 2 § polislagen.⁴² Senare har även 2 § polislagen ändrats så att uttryckssättet

⁴⁰ SFS 1998:622.

⁴¹ 2 § ändrades genom SFS 2014:588, prop. 2013/14:110 s. 126.

⁴² Se prop. 2009/10:85 s. 73–76.

brottslig verksamhet m.m. används. Ändringen avsåg inte att förändra polisens uppgifter i sak, utan var en anpassning till bl.a. den nya polisdatalagen.⁴³ Att någon motsvarande justering inte har gjorts i lagen om belastningsregister kan alltså knappast ges innebörden att de grundläggande ändamålen för polisens egen användning av registret skulle vara inskränkta i förhållande till ändamålen för behandling enligt polisdatalagen (eller i förhållande till beskrivningen av kärnverksamheten enligt 2 § polislagen).

Vi menar alltså att det inte går att identifiera några sakliga skäl till att ändamålen i lagen om belastningsregister ska vara annorlunda utformade än annan reglering på det brottsbekämpande området. Eftersom brottsdatalagen kommer att bli den centrala författningen inom detta område, bör ändamålen i lagen om belastningsregister omformuleras för att bättre överensstämja med de syften som är bestämmande för den lagens tillämpningsområde.

Information till den registrerade

Som vi anført i föregående avsnitt menar vi att det inte är förenligt med det nya dataskyddsdirektivet att ha kvar 9 § i lagen om belastningsregister som en särreglering i förhållande till brottsdatalagens krav på information. Den enskilde måste, med andra ord, kunna få information inte bara om vilka uppgifter som finns om honom eller henne i belastningsregistret, utan också den övriga information om behandlingen som följer av 4 kap. 3 § brottsdatalagen. En möjlighet att åstadkomma detta är att göra ett tillägg till bestämmelsen i 9 § första stycket som anger att även information i enlighet med brottsdatalagen ska lämnas då den enskilde begär ett registerutdrag. Ett annat sätt är att låta möjligheten att få ett registerutdrag enligt 9 § första stycket stå kvar och samtidigt i författningstexten förtydliga att den enskilde också kan begära information enligt 4 kap. 3 § brottsdatalagen. Den enskilde skulle då ha möjlighet att begära information både enligt 4 kap. 3 § brottsdatalagen och 9 § första stycket lagen om belastningsregister. För det fall en enskild först begärt information

⁴³ Prop 2013/14:110 s. 577.

enligt 9 § första stycket lagen om belastningsregister och sedan begär information enligt brottsdatalagen, skulle själva registerutdraget inte behöva lämnas ut en andra gång med tillämpning av 4 kap. 3 § andra stycket. Båda dessa lösningar skulle dock innebära en dubbelreglering av den enskildes rätt till information. En sådan dubbelreglering fyller egentligen inte någon funktion, vare sig för Polismyndigheten eller den enskilde. Vi förordar därför en annan lösning, som innebär att 9 § första stycket utgår ur lagen om belastningsregister. Möjligheten att få ett registerutdrag är för den enskilde densamma, men en begäran får i stället göras i enlighet med 4 kap. 3 § brottsdatalagen. Det kan tilläggas att det inte finns något som hindrar att Polismyndigheten ger den enskilde möjlighet att begära information om endast behandlingen i belastningsregistret och inte om andra personuppgifter som eventuellt behandlas av Polismyndigheten. Om en person inte är intresserad av någon annan information är det givetvis inte ändamålsenligt för vare sig den personen eller för Polismyndigheten att all tillgänglig information om behandling av personuppgifter lämnas.

Som vi tidigare redogjort för menar vi att de begränsade utdrag som den enskilde kan begära med stöd av 9 § andra och tredje styckena ska betraktas som en extra skyddsåtgärd i förhållande till det nya dataskyddsdirektivets krav på information. Sådana utdrag utgör alltså en särreglering i förhållande till brottsdatalagen och bör därför även fortsättningsvis regleras i lagen om belastningsregister.

Möjlighet till elektronisk identitetskontroll vid begäran om registerutdrag – 9 § fjärde stycket

Enligt 9 § fjärde stycket ska den som begär ett utdrag om sig själv ur belastningsregistret göra det genom en skriftlig begäran som undertecknas av den sökande. Utredningen om 2016 års dataskyddsdirektiv har redogjort för överväganden bakom kravet på egenhändigt undertecknande som finns i 26 § andra stycket personuppgiftslagen samt anfört skäl att göra regleringen teknikneutral, utan att behovet av en säker identifiering av den som gör en begäran eftersätts.⁴⁴ Vi anser att kravet på egenhändigt under-

⁴⁴ SOU 2017:29 s. 413–415.

tecknande av samma skäl kan utgå även när det gäller begäran om begränsade utdrag ur belastningsregistret. Den reglering som föreslås i brottsdataförordningen kommer att gälla med avseende på en begäran som görs enligt brottsdatalagen. Lagen om belastningsregister bör därför, liksom i dag, innehålla en egen reglering av kraven på en begäran om utdrag, men denna kan anpassas till vad som kommer att gälla enligt brottsdataförordningen.

Skadestånd och rättelse – 20 §

Som vi anför i våra allmänna överväganden (avsnitt 2.6.7) behövs inte någon hänvisning till bestämmelser om rättelse m.m. i brottsdatalagen för att dessa bestämmelser ska kunna tillämpas i stället för regleringen i personuppgiftslagen när denna lag upphävs. Det kan anmärkas att frågor om radering ur registret skulle kunna aktualiseras om ett avsnitt i registret är helt och hållet felaktigt, exempelvis med anledning av en personförväxling. Sådan radering är då möjlig med stöd av 4 kap. 9 §, eftersom raderingen i det fallet är det relevanta sättet att rätta personuppgiften.⁴⁵ Någon hänvisning till brottsdatalagen behövs inte för att den enskilde ska kunna begära rättelse i det avseendet.

Att det fanns lagkrav på rättelse av personuppgifter ansågs vid genomförandet av rambeslutet om kriminalregister (se vidare avsnitt 5.1) som en förutsättning för att rambeslutets krav i artikel 5.2 kunde anses genomförda utan författningsändringar.⁴⁶ Även när personuppgiftslagen upphävs kommer alltså rambeslutet vara genomfört i svensk rätt i denna del, utan några ytterligare författningsändringar.

Som vi tidigare redogjort för kommer dataskyddsförordningen att vara tillämplig på vissa behandlingar som avser utlämnande ur registret. Som vi också anført anser vi att förändret av registret dock faller under det nya dataskyddsdirektivets, och därmed brottsdatalagens, tillämpningsområde. Eftersom personuppgifternas korrekthet har att göra med vad som en gång förts in i registret kommer frågor om rättelse m.m. inte att bedömas enligt data-

⁴⁵ Se vidare SOU 2017:29 s. 405.

⁴⁶ Prop. 2011/12:163 s. 38 f.

skyddsförordningen. Detta gäller även om en eventuell felaktighet i registret skulle uppmärksammas i samband med ett utlämnande som i och för sig omfattas av dataskyddsförordningens tillämpningsområde.

För att 7 kap. 1 § brottsdatalagen om skadestånd ska gälla för behandling även enligt lagen om belastningsregister och föreskrifter med stöd av lagen behövs en hänvisning i lagen, se vidare våra allmänna överväganden, avsnitt 2.6.7.

Skadestånd enligt brottsdatalagen kan naturligtvis endast komma ifråga om skada orsakats vid behandling som omfattas av den lagens tillämpningsområde. Om skada uppkommit vid behandling som ska bedömas enligt dataskyddsförordningen blir förordningens skadeståndsreglering tillämplig. Som vi anført i våra generella överväganden behövs inga hänvisningar till dataskyddsförordningen för att åstadkomma detta.

Sanktionsavgifter

Som vi redogör för i våra allmänna överväganden (avsnitt 2.6.7) anser vi att det inte behöver införas särskilda bestämmelser om sanktionsavgifter i registerförfattningar som ingår i vårt uppdrag och som omfattas av det nya dataskyddsdirektivets tillämpningsområde. Inte heller i förhållande till dataskyddsförordningen behövs bestämmelser om sanktioner, se vidare avsnitt 2.5.9.

Bör gallringsbestämmelserna omformuleras?

Som vi tidigare nämnt (se avsnitt 2.6.3) anser Utredningen om 2016 års dataskyddsdirektiv att det är motiverat att i vissa registerförfattningar som omfattas av det nya dataskyddsdirektivets tillämpningsområde renodla terminologin när det gäller gallring och längsta tid för behandling av personuppgifter. I korthet anser utredningen att begreppet gallring inte bör användas i registerförfattningar. Skälet är att gallring är ett begrepp som används i arkivrättsliga sammanhang och att det ursprungliga syftet med att gallra är att begränsa omfattningen av de allmänna arkiven.⁴⁷

⁴⁷ SOU 2017:29 s. 282 f. och SOU 2017:74 s. 358.

När det gäller lagen om belastningsregister anser vi att det inte finns tillräckliga skäl att ändra i gallringsbestämmelserna, av följande skäl. Belastningsregistret innehåller uteslutande allmänna handlingar (som dock som utgångspunkt är sekretessbelagda). Gallringsbestämmelserna i lagen är utformade utifrån både integritetshänsyn och hänsyn till det samhällsliga intresset av att det finns information om enskildas brottsliga belastning. Samtidigt innebär gallringsbestämmelserna att det finns lagstöd för att just gallra allmänna handlingar. Ett byte av terminologi från *gallring* till exempelvis *längsta tid som uppgifterna får behandlas* skulle inte innebära något annat än just en förändring av bestämmelsernas ordalydelse samt ett behov av att se över gallringsbestämmelser i annan författning och eventuellt göra ändringar eller tillägg där. Vi anser att bestämmelserna om gallring just i lagen om belastningsregister är utformade på ett ändamålsenligt sätt och att de inte heller ger upphov till några tillämpningsproblem. Det finns därmed inte skäl att ändra deras ordalydelse.

Behövs bestämmelser som inskränker den enskildes rättigheter?

Som vi anfört i våra allmänna överväganden (avsnitt 2.6.6) finns inga generella skäl för oss att överväga inskränkningar i den registrerades rättigheter enligt det nya dataskyddsdirektivet. Våra slutsatser när det gäller den enskildes rätt till information enligt direktivet och den rättighetens förhållande till lagen om belastningsregister framgår av avsnitt 5.3.

Även om vissa utlämnanden ur belastningsregistret ska bedömas enligt dataskyddsförordningen blir det, som anförts ovan, inte aktuellt att tillämpa vissa bestämmelser i förordningen, eftersom själva insamlandet av personuppgifter till registret och bevarandet i registret regleras av det nya dataskyddsdirektivet. Frågor om information, rättelse och radering, som i förordningen regleras i artiklarna 13–17, regleras därmed av brottsdatalagen. Teoretiskt kan man dock tänka sig en tillämpning av rätten till begränsning av behandling och rätten att göra invändningar mot behandling, eftersom den enskilde skulle kunna vända sig emot just ett visst, eller en viss typ av utlämnande, för ett sådant ändamål som inte omfattas av det nya dataskyddsdirektivet och därmed regleras av

dataskyddsförordningen. Samtidigt är det svårt att föreställa sig att det någonsin skulle kunna bli fråga om att faktiskt begränsa behandlingen i enlighet med artikel 18 eller artikel 21. Eftersom utlämnanden är författningsreglerade, liksom alla de olika tillstånds- eller lämplighetsprövningar i vilka belastningsuppgifter kan behövas, måste det i praktiken bli nära nog omöjligt för den enskilde att åberopa några relevanta skäl. Det torde i de allra flesta fall vara tillräckligt för Polismyndigheten att hänvisa till författningsregleringen för att bemöta eventuella invändningar eller en begäran om begränsning, jfr vad vi anfört i våra allmänna överväganden, avsnitt 2.5.8. Vi anser därmed att det inte finns skäl att införa några bestämmelser som rör inskränkningar i den registrerades rättigheter enligt dataskyddsförordningen.

Slutligen ska anmärkas att om den registrerade begär rättelse av uppgifterna i registret i enlighet med 4 kap. 9 § brottsdatalagen och det inte genast går att fastställa om uppgifterna är korrekta eller inte, har Polismyndigheten en skyldighet enligt paragrafens andra stycke att begränsa behandlingen. En sådan begränsning torde omfatta utlämnanden eller annan behandling som i och för sig inte omfattas av brottsdatalagens tillämpningsområde. I vart fall kommer tekniska åtgärder för att begränsa behandlingen av praktiska skäl troligen att omfatta all vidare behandling, oavsett vilket regelverk som skulle varit tillämpligt på behandlingen om den utförts.

6 Lagen och förordningen om misstankeregister

6.1 Om författningarna

Bakgrund

Den nuvarande lagen (1998:621) och förordningen (1999:1135) om misstankeregister är, liksom lagen och förordningen om belastningsregister, en del av den reformerade lagstiftning om polisens register som genomfördes 1998 efter förslag av Registerutredningen. En utgångspunkt för lagstiftningsarbetet var att uppgifter om påföljder och uppgifter om misstankar om brott ska hållas åtskilda och inte behandlas inom samma register. Resultatet av utredningens förslag blev också skilda sådana register – belastningsregistret och misstankeregistret. Regleringen av de båda registren är dock i många avseende likadan.

Kort om författningarnas innehåll

Misstankeregistret innehåller uppgifter om den som har fyllt femton år och som enligt förundersökningsledarens bedömning är skäligen misstänkt för brott. Misstankeregistret innehåller även uppgifter om den mot vilken allmän åklagare har inlett utredning i mål om förvandling av böter och om den som har begärts överlämnad eller utlämnad för brott (3 §).

Strukturen och innehållet i lagen och förordningen om misstankeregister är, bortsett från att författningarna reglerar en annan typ av uppgifter, i princip överensstämmande med lagen och förordningen om belastningsregister. Polismyndigheten har alltså en skyldighet att föra misstankeregistret automatiserat och

myndigheten är personuppgiftsansvarig för behandlingen (1 §). Registrets ändamål (2 §) överensstämmer med ändamålen för belastningsregistret, med det undantaget att misstankeregistret inte används av domstol för straffmätning eller val av påföljd och inte heller av åklagare för utfärdande av strafföreläggande.

I övrigt innehåller lagen om misstankeregister bestämmelser om utlämnande ur registret (5–12 §§), gallring (13 §), tystnadsplikt (14 §) samt rättelse och skadestånd (15 §). Den enskildes rätt att få ett utdrag om sig själv regleras i 8 a § men avser endast den situationen att den enskilde behöver ett utdrag enligt bestämmelser i lagen (2007:171) om registerkontroll av personal vid vissa boenden som tar emot barn.

I förordningen om misstankeregister finns i huvudsak mer preciserade bestämmelser om vilka myndigheter och enskilda som har rätt att få utdrag ur registret (3–8 §§). Där finns också en mer detaljerad reglering av misstankeregistrets innehåll (2 §) och av vilka myndigheter som är skyldiga att lämna uppgifter till Polismyndigheten (10–13 §§).

Sekretess

Sekretess gäller för uppgifter i misstankeregistret om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till honom eller henne lider skada eller men om uppgiften röjs (35 kap. 1 § 7 offentlighets- och sekretesslagen [2009:400]).

6.2 Vilken EU-rättsakt är tillämplig?

Bedömning: Förändret av misstankeregistret och behandling i registret i brottsbekämpande syften omfattas av det nya dataskyddsdirektivets tillämpningsområde. På annan behandling av personuppgifter i registret, exempelvis för att lämna uppgifter som underlag för olika slag av lämplighets- och tillståndsprövningar, tillämpas dataskyddsförordningen.

Skälen för bedömningen:

Det nya dataskyddsdirektivet, dataskyddsförordningen eller båda?

Argumentationen om vilken EU-rättsakt som är tillämplig på behandlingen av personuppgifter enligt lagen och förordningen om belastningsregister kan i princip överföras till att gälla även för lagen och förordningen om misstankeregister. Vi hänvisar alltså till avsnitt 5.2 och redogör här för vår bedömning i korthet.

Misstankeregistret förs helt automatiserat och det innehåller personuppgifter. På behandlingen i registret är alltså antingen det nya dataskyddsdirektivet eller dataskyddsförordningen tillämplig. De båda rättsakterna kan inte vara tillämpliga samtidigt, dvs. på samma personuppgiftsbehandling. Däremot kan samma bestämmelse i någon av de svenska författningarna reglera behandling både inom det nya dataskyddsdirektivets tillämpningsområde och inom dataskyddsförordningens.

Vi har sett det som ändamålsenligt att först överväga vilken EU-rättsakt som ska tillämpas på *förandet av registret*. Bestämmelser i lagen och förordningen som reglerar registrets innehåll, bevarande i registret och gallring ur registret ska då bedömas utifrån denna EU-rättsakt. Frågor om rättelse m.m. som kan uppkomma avseende innehållet i registret ska också bedömas på grundval av den EU-rättsakt som är tillämplig på förandet av registret.

Polismyndigheten är en behörig myndighet i det nya dataskyddsdirektivets mening. Även om flera ändamål med misstankeregistret pekas ut i 2 § i lagen, menar vi att det grundläggande syftet med att föra ett register är de brottsbekämpande ändamål som anges i 2 § första stycket 1 och 2. Förandet av registret omfattas därmed av det nya dataskyddsdirektivets tillämpningsområde. Behandling i registret för att tillgodose brottsbekämpande myndigheters behov att ta del av uppgifterna för sådana syften omfattas också av direktivet.

När det gäller behandling i registret för olika tillstånds- och lämplighetsprövningar är syftet däremot inte att bekämpa brott i det nya dataskyddsdirektivets mening, även om man kan argumentera för att sådana prövningar har betydelse för att förebygga brott i vid bemärkelse. Behandling för att utlämna uppgifter ur registret för sådana syften omfattas därmed av dataskyddsförordningens tillämpningsområde. Även Polismyndighetens egen

användning av registret för sådana syften omfattas av dataskyddsförordningen.

Vår bedömning av personuppgiftsbehandlingen i misstankeregistret överensstämmer med den som Utredningen om 2016 års dataskyddsdirektiv har gjort.¹

Vilken behandling omfattas av dataskyddsförordningen respektive det nya dataskyddsdirektivet?

Behandling i misstankeregistret i enlighet med de ändamål som anges i 2 § första stycket 1 och 2 avser behandling för syften inom det nya dataskyddsdirektivets tillämpningsområde. Polismyndighetens utlämnanden till andra svenska myndigheter för sådana ändamål i enlighet med 5 § första stycket 1 omfattas därmed av direktivet.

När det gäller uttag ur registret för sådana lämplighets-, tillstånds- och andra prövningar som avses i 2 § första stycket 3 är det i många fall i stället dataskyddsförordningen som är tillämplig, eftersom syftet med sådana uttag ofta inte omfattas av direktivet. Av de utlämnanden som regleras i 3–7 §§ i förordningen om misstankeregister torde följande utlämnanden omfattas av det nya dataskyddsdirektivets tillämpningsområde.²

- utlämnanden för ärenden som rör brott eller straffverkställighet till det statsråd som är föredragande i ärendet (delar av 3 § 1, motsvaras av delar av 10 § första stycket 1 förordningen om belastningsregister)
- utlämnande till migrationsdomstol eller Migrationsöverdomstolen i mål om upphävande av allmän domstols beslut om utvisning på grund av brott (3 § 10, motsvaras av 10 § första stycket 20 förordningen om belastningsregister)
- utlämnanden till Kriminalvården för prövningar enligt fängelselagen (2010:610), lagen (1994:451) om intensivövervakning med elektronisk kontroll, lagen (1991:2041) om särskild personutredning i brottmål m.m., (delar av 4 § 3, motsvaras av delar av 10 § första stycket 10 förordningen om belastningsregister),

¹ SOU 2017:29 s. 216.

² För hänvisningar till bedömningar gjorda i SOU 2017:29, se motsvarande uppställning i avsnitt 5.2.

- utlämnande till en övervakningsnämnd eller Kriminalvården, i ärenden om övervakning (4 § 4, motsvaras av 10 § första stycket 11 förordningen om belastningsregister).

Vissa utlämnanden som föreskrivs i förordningen om misstankeregister får bedömas från fall till fall, beroende på det mer specifika syftet med varje utlämnande. Det gäller åklagarmyndighetens tillgång till uppgifter enligt 3 § 2 (motsvaras av 10 § första stycket 3 förordningen om belastningsregister) som kan gälla frågor om tillträdesförbud och kontaktförbud, som omfattas av det nya dataskyddsdirektivets tillämpningsområde. När det gäller prövningar som Kriminalvården gör enligt häkteslagen (2010:611) beror det på om den person prövningen gäller är frihetsberövad p.g.a. (misstanke om) brott eller av någon annan orsak (del av 4 § 3, motsvaras av del av 10 § 10 förordningen om belastningsregister). Häkteslagen är nämligen tillämplig även på vissa andra frihetsberövanden än anhållande, häktning eller verkställighet eller ändring av påföljd.

Utlämnande för statistiska ändamål (7 § i lagen, motsvaras av 8 § lagen om belastningsregister) omfattas av dataskyddsförordningens tillämpningsområde, liksom utlämnanden till enskilda enligt 8 § (motsvaras av 10 § lagen om belastningsregister).

När det gäller utlämnanden genom direktåtkomst får det avgöras från fall till fall om utlämnanden sker för syften som omfattas av det nya dataskyddsdirektivet eller av förordningen.

När det gäller utlämnande till utländska myndigheter framgår det av lagen om misstankeregister att utlämnanden till utländska polis- eller åklagarmyndigheter inom Interpol i huvudsak sker för brottsbekämpande ändamål (10 §, motsvaras av 12 § andra stycket lagen om belastningsregister). Utlämnanden enligt 9 § i lagen får bedömas utifrån det syfte som kan utläsas ur den internationella överenskommelsen som är aktuell i det enskilda fallet (9 § motsvaras av 11 § lagen om belastningsregister).

6.3 Överväganden om befintliga bestämmelser i förhållande till det nya dataskyddsdirektivet

Bedömning: Bestämmelserna i 1, 2–7, 8 a–13 §§ i lagen om misstankeregister, 1–4, 6, 8 a, 10–18 §§ i förordningen om misstankeregister är bestämmelser som helt eller delvis får betydelse för personuppgiftsbehandling inom det nya dataskyddsdirektivets tillämpningsområde. Bestämmelserna behöver inte ändras som en följd av att dataskyddsdirektivet ska genomföras i svensk rätt. Bestämmelserna i 1 a, 1 b och 15 §§ i lagen behöver upphävas eller ändras som en följd av att personuppgiftslagen och lagen (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen kommer att upphävas.

Skälen för bedömningen:

Inledning

I detta avsnitt görs en genomgång av de bestämmelser i lagen och förordningen om misstankeregister som reglerar personuppgiftsbehandling inom det nya dataskyddsdirektivets tillämpningsområde. Som framgår anser vi att de flesta bestämmelser kan behållas oförändrade och vi redovisar här skälen för denna bedömning. I de fall vi identifierat behov av förändringar anges skälen även för detta. Våra förslag till förändringar och skälen till att vi utformat dem på ett visst sätt framgår sedan av avsnitt 6.5.

Utgångspunkten för våra överväganden är alltså, som vi redogjort för ovan, att den automatiserade personuppgiftsbehandling som förändret av registret innebär omfattas av det nya dataskyddsdirektivet. För att dataskyddsdirektivet ska bli korrekt genomfört avseende behandlingen i misstankeregistret måste därmed brottsdatalagen tillämpas, eftersom lagen om misstankeregister i sig inte reglerar alla de områden som ingår i direktivet. I våra överväganden nedan utgår vi alltså ifrån att brottsdatalagen är tillämplig på personuppgiftsbehandling som regleras av lagen och förordningen om misstankeregister. Våra förslag till hur detta förhållande ska författningsregleras och vilka följdändringar det för

med sig följer i avsnitt 6.5. När vi analyserar bestämmelserna i lagen och förordningen om misstankeregister utgår vi dock i första hand från direktivets reglering, eftersom vi uppfattat vårt uppdrag så att vi ska göra en självständig analys av de ingående författningarnas förhållande till EU-rättsakterna, samtidigt som vi givetvis ska förhålla oss till andra utredningars författningsförslag som får betydelse för tillämpningen av de författningar som ingår i vårt uppdrag.

Skyldigheten att föra registret, personuppgiftsansvar, registrets ändamål och innehåll

Att Polismyndigheten åläggs att föra ett misstankeregister innebär att myndigheten uttryckligen getts en uppgift som omfattas av de syften som ingår i direktivets tillämpningsområde. Bestämmelsen i 1 § är alltså förenlig med dataskyddsdirektivet och genomför kravet på att behandling ska vara laglig (artikel 8).

Att Polismyndigheten pekas ut som personuppgiftsansvarig i 1 § är också förenligt med direktivet (se vidare avsnitt 2.6.3). Att det finns en bestämmelse som reglerar att det är Polismyndigheten som prövar frågor om utlämnande (12 §) får ses som en precisering av vad som ingår i uppgiften att föra registret och i personuppgiftsansvaret. Bestämmelserna behöver alltså inte ändras p.g.a. direktivet.

Av artikel 8 i direktivet framgår att ändamål med behandlingen och vilka personuppgifter som får behandlas ska regleras i nationell rätt. Bestämmelserna i 2–4 §§ i lagen, som rör registrets ändamål och innehåll, är alltså även de förenliga med direktivet. Detsamma gäller 2 § i förordningen som avser registrets innehåll. Bestämmelsen i 1 § i förordningen är endast av upplysande karaktär och påverkas därmed inte av direktivet. I 10–13 §§ i förordningen specificeras vilka myndigheter som ska lämna uppgifter till Polismyndigheten för införande i registret. Myndigheterna i fråga har uppdrag att lagföra brott och verkställa straffrättsliga påföljder. Uppgiftsskyldigheten innebär indirekt en reglering av misstanke- registrets innehåll och är förenlig med dataskyddsdirektivet.

Känsliga personuppgifter

Rubriceringen på det brott som en misstanke avser skulle i vissa fall kunna betraktas som en känslig personuppgift, exempelvis då rubriceringen gäller sexualbrott.³ Att vissa känsliga personuppgifter kan komma att behandlas i misstankeregistret får anses förenligt med artikel 10 i det nya dataskyddsdirektivet. Kraven enligt artikel 10 är att sådan behandling ska följa av nationell rätt, vara absolut nödvändig och att det ska finnas lämpliga skyddsåtgärder. Samtliga dessa krav får anses uppfylla. Den utförliga författningsregleringen av misstankeregistret får anses i sig utgöra en skyddsåtgärd, liksom tillämpliga sekretessbestämmelser. Det är absolut nödvändigt för syftet med behandlingen att behandla uppgifter om brottsrubricering i misstankeregistret.

Direktivets artikel 10 har genomförts i 2 kap. 11 § brottsdatalagen. Förutsättningarna för att behandla sådana uppgifter skiljer sig något från direktivets utformning, men behandlingen i misstankeregistret av sådana uppgifter får anses vara förenlig även med bestämmelsen i brottsdatalagen. Vi återkommer i avsnitt 6.5 med förslag i anledning av den sökbegränsning för känsliga personuppgifter som föreskrivs i brottsdatalagen (2 kap.14 §).

Förhållandet till annan reglering av personuppgiftsbehandling

I 1 a och b §§ regleras för närvarande förhållandet till personuppgiftslagen och lagen (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen. Som vi redogör för i avsnitt 5.3 kommer båda dessa lagar upphävas som en följd av EU:s dataskyddsreform. Bestämmelserna i 1 a och b §§ måste alltså ändras och anpassas till detta förhållande. Vi återkommer med våra förslag till ändringar i avsnitt 6.5.

³ SOU 2017:74 s. 872.

Bestämmelser om utlämnande ur registret till svenska myndigheter

I 5 § lagen om misstankeregister finns de grundläggande bestämmelserna om svenska myndigheters möjlighet att få tillgång till uppgifter i misstankeregistret. Som redan redogjorts för kommer inte alla utlämnanden ur registret att omfattas av det nya dataskyddsdirektivets tillämpningsområde, se ovan, avsnitt 6.2. I förordningen om misstankeregister specificeras ytterligare möjligheten att få ut uppgifter. Det är endast vissa utlämnanden i 3 och 4 §§ samt regleringen av direktåtkomst i 6 § som avser brottsbekämpande ändamål.

Att specificera vilka uppgifter som får lämnas ut och i vilka fall får anses förenligt med det nya dataskyddsdirektivet. Den särskilda regleringen av direktåtkomst i 6 § är också förenlig med direktivet, se vidare våra allmänna överväganden, avsnitt 2.6.3.

Den reglering som avser utlämnanden ur registret för andra syften än brottsbekämpning etc. tar vi upp i nästa avsnitt (avsnitt 6.4). Att uppgifter som först behandlats inom det nya dataskyddsdirektivets tillämpningsområde senare behandlas för andra syften är förenligt med dataskyddsdirektivet om sådan vidarebehandling är reglerad i nationell rätt eller unionsrätten (artikel 9). Författningsregleringen av sådant utlämnande genomför alltså även direktivets krav.

Polismyndighetens utlämnande av uppgifter ur registret till andra svenska myndigheter, både brottsbekämpande sådana och andra, är reglerad som en uppgiftsskyldighet (uppgifterna ska lämnas ut om de begärs, 5 § i lagen). Redan av denna anledning blir det inte aktuellt att göra någon prövning enligt 2 kap. 4 § (eller 2 kap. 22 §) brottsdatalagen.

Särskilt om Polismyndighetens användning av uppgifter i registret för myndighetens egen brottsbekämpande verksamhet

Att Polismyndigheten kan använda misstankeregistret för brottsbekämpande syften regleras inte på annat sätt i lagen om misstankeregister än genom att denna användning omfattas av registrets ändamål i 2 § första stycket 1. Vi har i avsnitt 5.3 diskuterat om man ska bedöma Polismyndighetens behandling i belastningsregistret för behov inom den egna verksamheten för något av de

ändamål som anges i 2 § första stycket 1 i den lagen, som motsvarar ändamålsbestämmelsen i lagen om misstankeregister, som behandling för ett *nytt ändamål* i det nya dataskyddsdirektivets och brottsdatalagens mening. I sådana fall skulle direktivet, som i denna del genomförs i 2 kap. 4 § brottsdatalagen, ställa särskilda krav på att behandlingen ska vara nödvändig och proportionerlig för att vara tillåten. Vår slutsats är att behandling i enlighet med de ändamål som anges i 2 § första stycket 1 lagen om belastningsregister inte bör anses vara för ett nytt ändamål och att 2 kap. 4 § brottsdatalagen därmed inte ska tillämpas. Vi gör samma bedömning när det gäller Polismyndighetens behandling för sådana ändamål i misstankeregistret. För en utförligare redogörelse hänvisar vi till avsnitt 5.3.

Det kan anmärkas att lagen och förordningen om misstankeregister enbart reglerar förande och behandling av uppgifterna i registret, i förekommande fall utlämnanden av uppgifterna. När uppgifter om en person ”lämnat” registret och vidarebehandlas för exempelvis en brottsutredning, eller för något annat brottsbekämpande ändamål, blir andra regelverk tillämpliga beroende på vilken verksamhet den fortsatta behandlingen sker i.

Intresseavvägning före utlämnande

I 6 § finns en bestämmelse som berör alla svenska myndigheter som har möjlighet att få uppgifter ur registret. Bestämmelsen innebär att en myndighet alltid ska göra en intresseavvägning mellan skälet för begäran å ena sidan och den olägenhet eller det men en begäran innebär för den enskilde å den andra. Samma intresseavvägning finns i 7 § lagen om belastningsregister. Vi har när det gäller 7 § lagen om belastningsregister kommit fram till att bestämmelsen är förenlig med det nya dataskyddsdirektivet. Vi gör samma bedömning avseende 6 § lagen om misstankeregister. För en utförligare diskussion, se avsnitt 5.3.

Utlämnande till den registrerade

Den som är registrerad i misstankeregistret kan, enligt 8 a § i lagen (som preciseras i 8 a § i förordningen), få ett registerutdrag beträffande sig själv om det behövs enligt bestämmelser i lagen (2007:171) om registerkontroll av personal vid vissa boenden som tar emot barn. Möjligheten att få ett sådant särskilt anpassat registerutdrag får betraktas som ett skydd för den enskildes integritet – registerutdraget är begränsat så att inte mer information om den enskilde ska framgå än vad som är nödvändigt med beaktande av syftet med utdraget.⁴ Denna särskilda informations-skyldighet i förhållande till den registrerade strider inte mot det nya dataskyddsdirektivet, eftersom direktivet under alla förhållanden tillåter starkare skyddsåtgärder.

Om den enskilde begär allmän information om vilka personuppgifter som behandlas om honom eller henne med stöd av 4 kap. 3 § brottsdatalagen får denna begäran när det gäller uppgifter i misstankeregistret prövas i enlighet med brottsdatalagens reglering och gällande sekretessbestämmelser.⁵

Bestämmelser om utlämnande till utländska myndigheter

Utlämnande ur misstankeregistret till utländska myndigheter i brottsbekämpande syften regleras i huvudsak i 10 § i lagen om misstankeregister, men även utlämnanden i enlighet med 9 § skulle kunna omfattas av det nya dataskyddsdirektivet beroende på syftet med utlämnanden. Som redan anförts förhindrar inte det nya dataskyddsdirektivet en närmare nationell reglering av utlämnande-frågor. Detta ställningstagande förändras inte av att regleringen gäller utländska myndigheter.

När det gäller gränsöverskridande utbyte av personuppgifter som innebär en automatiserad behandling finns en särskild reglering av överföring till tredje land och internationella organisationer i det nya dataskyddsdirektivet. Direktivet genomförs i detta avseende i 8 kap. brottsdatalagen. Bestämmelserna om utlämnande i lagen om misstankeregister möjliggör ett uppgiftsutlämnande till

⁴ Jfr prop. 2006/07:37 s. 17 f.

⁵ Jfr dock SOU 2017:29 s. 384.

tredje land genom att uppgiftsutbyte tillåts ske med Interpol och länder anslutna till Interpol. Om personuppgifterna behandlas helt eller delvis automatiserat för att överföras till tredje land måste de förutsättningar som följer av 8 kap. brottsdatalagen också vara uppfyllda för att överföringen ska kunna ske. Regleringen av tredjelandsöverföringar i 33–35 §§ personuppgiftslagen ersätts alltså, såvitt avser överföring för de syften som omfattas av direktivet, av 8 kap. brottsdatalagen.⁶

Gallring

Som anförts i våra allmänna överväganden (avsnitt 2.6.3) hindrar inte det nya dataskyddsdirektivet att tidsfrister för bevarande regleras i författning. Enligt direktivet är det t.o.m. en skyldighet för medlemsstaterna att bestämma närmare tidsfrister för radering och lagring (artikel 5). De bestämmelser som rör gallring i lagen om misstankeregister kan alltså i och för sig behållas (13 §).

I nästa avsnitt överväger vi om det annars finns skäl att förändra ordalydelsen av de nuvarande gallringsbestämmelserna med hänsyn till de förslag som Utredningen om 2016 års dataskyddsdirektiv lämnar när det gäller frågor om gallring och längsta tid för behandling av personuppgifter.

Rättelse och skadestånd

Bestämmelsen i 15 § hänvisar till personuppgiftslagen och måste därför anpassas till att denna lag upphör och att brottsdatalagen i stället ska tillämpas. Vi lämnar förslag i avsnitt 6.5.

Ansvar för lämnade uppgifter

I 14 och 15 §§ i förordningen finns bestämmelser om ansvar för lämnade uppgifters riktighet och rättelse av felaktiga uppgifter. Bestämmelserna avser felaktigheter som upptäcks av de inblandade myndigheterna och alltså inte den enskildes rätt till rättelse. Såvitt

⁶ Jfr prop. 2009/10:85 s. 203, jfr s. 321 och s. 330.

avser behöriga myndigheter, vars uppgiftslämnande omfattas av direktivets tillämpningsområde, kan bestämmelserna ses som preciseringar av principen om att personuppgifter ska vara korrekta (artikel 4.1 d som genomförs i 2 kap. 7 § brottsdatalagen). Förordningens bestämmelser kan därmed anses genomföra direktivet i denna del och utgör en precisering i förhållande till bestämmelsen i brottsdatalagen. De kan och bör därför behållas i förordningen.

Föreskriftsrätt

I 4 och 11 §§ i lagen och 16–18 §§ i förordningen finns bestämmelser om föreskriftsrätt. Bestämmelserna påverkas inte av det nya direktivet, se vidare våra allmänna överväganden, avsnitt 2.6.3.

6.4 Överväganden om befintliga bestämmelser i förhållande till dataskyddsförordningen

Bedömning: Bestämmelserna i 5–8, 9–11 och 14 §§ i lagen om misstankeregister samt 3–8 §§ i förordningen om misstankeregister avser, helt eller delvis, behandling av personuppgifter inom dataskyddsförordningens tillämpningsområde. Bestämmelserna är förenliga med förordningen och några författningsändringar behöver inte göras till följd av att förordningen börjar tillämpas.

Skälen för bedömningen:

Inledning

Vi har tidigare konstaterat att förändret av misstankeregistret får anses omfattas av det nya dataskyddsdirektivets tillämpningsområde. Att dataskyddsförordningen också blir tillämplig på viss behandling i registret beror på att ändamålet med en del behandling i registret inte avser brottsbekämpning, lagföring eller något annat av de ändamål som avses i artikel 2.1 d i dataskyddsförordningen och artikel 1.1 i det nya dataskyddsdirektivet.

I detta avsnitt bedömer vi de bestämmelser som vi menar reglerar behandling inom dataskyddsförordningens tillämpningsområde. Samma bestämmelser kan vara tillämpliga även på behandling inom det nya dataskyddsdirektivets område. Följden av att behandlingen i misstankeregistret ibland omfattas av dataskyddsförordningens, ibland av det nya dataskyddsdirektivets tillämpningsområde är alltså att vissa bestämmelser måste bedömas utifrån båda EU-rättsakternas krav.⁷

Vi bedömer att det är 5–8, 9–11 och 14 §§ i lagen om misstankeregister samt 3–8 §§ i förordningen om misstankeregister som innehåller de bestämmelser som ska bedömas med beaktande av dataskyddsförordningen. Som följer av våra överväganden nedan anser vi att bestämmelserna är förenliga med förordningen.

Myndigheters tillgång till uppgifter i misstankeregistret

Att Polismyndigheten gör uttag ur misstankeregistret för att lämna dem till andra myndigheter för prövningen i tillstånds- och lämplighetsfrågor eller för myndighetens egna prövningar för sådana ändamål får anses vara behandling för att utföra en uppgift av allmänt intresse (artikel 6.1 e). Utlämnandena är reglerade i författning, liksom de prövningar i sig som uppgifterna ur misstankeregistret behövs för. Kraven på rättslig grund och att denna ska vara fastställd i nationell rätt (artikel 6.1 och 6.3) är alltså uppfyllda.

Det kan tilläggas att när det gäller visst uppgiftsutbyte inom EU får personuppgiftsbehandlingen även anses ha rättsliga grunder som fastställts i unionsrätten. Det gäller exempelvis utlämnande med stöd av 5 a § i förordningen, som avser prövningar av Tullverket i enlighet med Europaparlamentets och rådets förordning (EU) nr 952/2013 av den 9 oktober 2013 om fastställande av en tullkodex för unionen och de förordningar som meddelas med stöd av den förordningen.

Att författningsregleringen tydligt preciserar i vilka fall och för vilka ändamål utlämnanden får ske är vidare förenligt med artikel 6.2 och 6.3. Bestämmelserna i 5 § lagen om misstankeregister är därmed förenliga med dataskyddsförordningen, liksom de ytter-

⁷ Jfr Fi2017/02899/S3 s. 124 f.

ligare preciseringar av utlämnande som finns i 3–7 §§ i förordningen om misstankeregister. Som vi redan berört reglerar bestämmelserna i förordningen endast delvis utlämnanden för syften som omfattas av dataskyddsförordningens tillämpningsområde. Även när det gäller 6 § berörs den endast av dataskyddsförordningen i den mån direktåtkomsten kan utnyttjas för andra ändamål än brottsbekämpning etc.

Även regleringen i 7 § i lagen om misstankeregister som möjliggör utlämnande för statistiska ändamål är, i enlighet med det ovan anförda, förenlig med dataskyddsförordningen. Vi menar att det inte ingår i vårt uppdrag att analysera om de särskilda förutsättningarna i artikel 89 avseende behandling för statistiska ändamål är uppfyllda, eftersom denna behandling i sig inte regleras av lagen om misstankeregister.⁸

För den reglering som möjliggör utlämnande till utländska myndigheter (9 och 10 §§ i lagen) för ändamål inom dataskyddsförordningens tillämpningsområde gäller också de ovan gjorda bedömningarna – författningsregleringen kan ses som fastställandet av en rättslig grund för utlämnanden och därtill en tillåten precisering av i vilka situationer behandling är tillåten. Man får utgå från att utlämnanden som ligger inom ramen för internationella överenskommelser eller EU-rättsakter (9 §) har ett allmänintresse som grund eller att personuppgiftsbehandling till följd av överenskommelsen eller EU-rättsakten är en rättslig förpliktelse.

Om utlämnanden som inte avser brottsbekämpning skulle komma i fråga till ett tredje land ska dataskyddsförordningens särskilda reglering av sådana utlämnanden tillämpas, om utlämnandet innebär en helt eller delvis automatiserad behandling, jfr vad som sagts ovan om utlämnanden till tredje land inom brottsdatalagens tillämpningsområde.

⁸ Det kan dock noteras att behandlingen är författningsreglerad i förordningen (2001:100) om den officiella statistiken och därtill omgärdad av vad som får betraktas som skyddsåtgärder för den enskilde i och med gällande sekretessreglering i 24 kap. 8 § första stycket offentlighets- och sekretesslagen (2009:400).

Intrasseavvägningen enligt 6 §

I 6 § finns, som tidigare beskrivits, en bestämmelse som innebär en skyldighet för en myndighet som begär ut uppgifter ur registret att alltid göra en avvägning mellan behovet av information och den enskildes intresse av att uppgifter *inte* inhämtas. Bestämmelsen riktar sig alltså till samtliga myndigheter som har möjlighet att få uppgifter ur registret, även myndigheter som inte är att anse som behöriga i det nya dataskyddsdirektivets mening. Bestämmelsen motsvaras av 7 § lagen om belastningsregister. Vi gör samma bedömning avseende 6 § lagen om misstankeregister som när det gäller 7 § lagen om belastningsregister, se vidare avsnitt 5.4. Bestämmelsen är alltså förenlig med dataskyddsförordningen.

Polismyndighetens användning av uppgifter för ändamål utanför brottsdatalogens tillämpningsområde

På samma sätt som när det gäller belastningsregistret blir 2 kap. 22 § brottsdatalogen tillämplig om Polismyndigheten söker uppgifter i registret för att de behövs för myndighetens egen verksamhet för ändamål utanför brottsdatalogens tillämpningsområde, se avsnitt 5.4 för en utförligare redogörelse. Vi återkommer i avsnitt 6.5 till frågan om detta är en lämplig ordning.

Utlämnande till enskilda

Enskilda kan få ta del av uppgifter om andra enskilda i misstankeregistret. Det gäller dels i vissa anställningsärenden, dels om en enskild kan styrka att hans eller hennes rätt är beroende av uppgifterna i fråga (8 § i lagen). Vilka anställningsärenden det kan vara fråga om preciseras i 8 § i förordningen.

Regleringen av enskildas rätt att ta del av uppgifter ur misstankeregistret överensstämmer med regleringen i 10 § i lagen och 21 § i förordningen om belastningsregister. I lagen om misstankeregister finns, liksom i lagen om belastningsregister, en bestämmelse om tystnadsplikt (14 §). Vi hänvisar därför till våra överväganden i avsnitt 5.4. Vi har där gjort bedömningen att regleringen är förenlig med dataskyddsförordningen och vi gör

samma bedömning när det gäller regleringen i lagen och förordningen om misstankeregister.

Slutligen ska nämnas att avgift tas ut för utdrag som begärs av enskilda (9 § i förordningen). Bestämmelsen avser inte en reglering av personuppgiftsbehandlingen i sig och påverkas därmed inte av dataskyddsförordningen.

Behandling av personnummer och känsliga personuppgifter

Även när det gäller behandling av personnummer är författningsregleringen i 2 § i förordningen om misstankeregister densamma som i 2 § förordningen om belastningsregister. Eftersom personnummer ingår i uppgifterna i registret kommer sådana att behandlas både inom det nya dataskyddsdirektivets och dataskyddsförordningens tillämpningsområde. Vidare kan, på samma sätt som inom det nya dataskyddsdirektivets tillämpningsområde, vissa uppgifter i misstankeregistret kunna betraktas som känsliga personuppgifter, se föregående avsnitt. Som vi argumenterat för i avsnitt 5.4 är behandling av personnummer och känsliga personuppgifter i belastningsregistret för ändamål inom dataskyddsförordningens tillämpningsområde förenlig med förordningen. Av samma skäl är sådan behandling i misstankeregistret förenlig med dataskyddsförordningen.

6.5 Överväganden om och förslag till författningsändringar

Förslag: I lagen om misstankeregister ges 1 a § ett nytt innehåll som anger att lagen gäller utöver brottsdatalagen. Vidare införs en bestämmelse i paragrafen som anger att sökbegränsningen i 2 kap. 14 § brottsdatalagen inte hindrar sökningar på brottsrubricering. Den nuvarande bestämmelsen i 1 b § upphävs och i stället införs en ny paragraf (en ny 1 b §) som anger att lagens bestämmelser kompletterar dataskyddsförordningens reglering i vissa fall.

Ändamålen med misstankeregistret i 2 § anpassas till brottsdatalagens terminologi såvitt avser de brottsbekämpande myndigheternas användning av registret.

Kravet på egenhändigt undertecknande av en begäran om utdrag enligt 8 a § andra stycket ersätts med att Polismyndigheten ska säkerställa att begäran har gjorts av en behörig person.

Bestämmelsen i 15 § ändras så att en hänvisning görs till brottsdatalagens bestämmelser om skadestånd. Hänvisningen till personuppgiftslagen tas bort.

Bedömning: Bestämmelserna om gallring bör stå kvar oförändrade. Några bestämmelser som avser inskränkning i den registrerades rättigheter enligt det nya dataskyddsdirektivet eller dataskyddsförordningen behövs inte. Bestämmelser om sanktionsavgifter behövs inte.

Skälen för förslaget och bedömningen:

Förhållandet till annan lagstiftning – 1 a och 1 b §§

Som tidigare angetts måste 1 a § ändras eftersom den hänvisar till personuppgiftslagen, som kommer att upphävas som en följd av den nya EU-regleringen. Bestämmelsen i 1 b § hänvisar till en annan författning som kommer att upphävas – lagen (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polis-samarbete och straffrättsligt samarbete inom Europeiska unionen. I lagen om misstankeregister bör i stället införas bestämmelser som klargör förhållandet till den generella reglering av personuppgifts-behandling som kommer att bli gällande – brottsdatalagen, data-skyddsförordningen och dataskyddslagen.⁹

Liksom andra registerförfattningar som gäller inom det nya dataskyddsdirektivets tillämpningsområde bör det anges att lagen om misstankeregister gäller *utöver* brottsdatalagen, se vidare avsnitt 2.6.7.

När det gäller sökbegränsningen avseende känsliga personuppgifter i 2 kap 14 § brottsdatalagen menar vi att vissa undantag

⁹ Upphävande av 1 b § föreslås också av Utredningen om 2016 års dataskyddsdirektiv som en följd av utredningens förslag att 2013 års lag ska upphävas, se SOU 2017:74 s. 73.

bör göras. Denna fråga behandlas vidare nedan. Som vi diskuterat ovan (avsnitt 6.3) skulle en viss tveksamhet kunna uppstå om tillämpningen av 2 kap. 4 § brottsdatalagen i förhållande till Polismyndighetens uttag ur misstankeregistret för brottsbekämpande ändamål. Vi menar dock att det inte finns behov av att införa någon författningsreglering som avser denna fråga, utan att den kan klargöras tillräckligt i författningskommentaren.

När det gäller dataskyddsförordningen anser vi att det bör anges som en upplysning att lagen kompletterar förordningen (se vidare våra generella överväganden, avsnitt 2.5.9). Man hade i och för sig kunnat helt undvara en hänvisning till dataskyddsförordningen med motiveringen att det framgår av brottsdatalagen i sig att vissa behandlingar av uppgifter, som från början samlats in och behandlats inom tillämpningsområdet för brottsdatalagen, sedermera kan komma att behandlas för syften som gör dataskyddsförordningen tillämplig i stället (2 kap. 22 §)¹⁰. Vi menar dock att det kan vara befogat att ha en sådan bestämmelse även i lagen om misstankeregister, så att det redan av den lagen framgår att behandlingen i registret kan komma att omfattas antingen av brottsdatalagens eller dataskyddsförordningens tillämpningsområde.

I den upplysande bestämmelsen som tar upp dataskyddsförordningen bör också anges att dataskyddslagen gäller, se vidare våra överväganden om behovet av författningsreglering av förhållandet mellan registerförfattningar och dataskyddslagen, avsnitt 2.5.9.

Undantag från sökbegränsningen för känsliga personuppgifter

Utredningen om 2016 års dataskyddsutredning föreslår för de flesta registerförfattningar som gäller för behöriga myndigheters personuppgiftsbehandling att det ska göras vissa undantag från sökbegränsningen avseende känsliga personuppgifter som följer av 2 kap. 14 § brottsdatalagen.¹¹ Undantagen omfattar bl.a. möjligheten att söka på brottsrubriceringar. Det finns behov av att kunna söka på brottsrubriceringar i misstankeregistret och därför uppstår samma behov att göra undantag från brottsdatalagens sökbegränsning även i misstankeregistret.

¹⁰ 2 kap. 21 § enligt förslaget i SOU 2017:29, ändrad till 2 kap. 22 § i SOU 2017:74, se s. 190 f.

¹¹ Se exempelvis förslaget till 2 kap. 5 § polisens brottsdatalag (s. 97 i SOU 2017:74) och överväganden till förslaget (a. a. s. 423–426).

Proportionalitetsprövningen enligt 2 kap. 22 § brottsdatalagen

Vi har i avsnitt 5.5 fört en diskussion om hur man kan se på tillämpningen av 2 kap. 22 § i förhållande till Polismyndighetens användning av uppgifter i belastningsregistret. Argumentationen är direkt överförbar på misstankeregistret och vi hänvisar därför till avsnitt 5.5. Vi lämnar inget förslag på undantag från 2 kap. 22 § såvitt avser behandling i belastningsregistret och vi lämnar följaktligen inte något förslag på undantag när det gäller misstankeregistret. I korthet anser vi att det finns argument både för och emot att 2 kap. 22 § ska tillämpas av Polismyndigheten såvitt avser behandling för ändamål utanför brottsdatalagens tillämpningsområde, men att frågan lämpligen bör övervägas vidare inom det fortsatta lagstiftningsarbetet avseende brottsdatalagen och polisens brottsdatalag.

Justering av ändamålen med misstankeregistret

Vi ger i andra avsnitt i denna promemoria uttryck för att vi tror att det kan underlätta för myndigheter som har att tillämpa flera olika författningar som rör personuppgiftsbehandling att författningarna använder sig av samma reglering och samma uttryckssätt så långt det är möjligt och om det inte finns sakliga skäl emot en sådan ordning. Med utgångspunkt i detta synsätt har vi i avsnitt 5.5 övervägt om ändamålen för belastningsregistret som avser brottsbekämpning ska omformuleras för att bättre överensstämma med det uttryckssätt som används i brottsdatalagen för att avgränsa den lagens tillämpningsområde. Argumentationen är direkt överförbar på lagen om misstankeregister, vars ändamål i 2 § första stycket 1 är formulerade på samma sätt som ändamålen för belastningsregistret i denna del. Vi menar alltså att även ändamålen för misstankeregistret bör ändras på samma sätt som ändamålen för belastningsregistret.

Möjlighet till elektronisk identitetskontroll vid begäran om registerutdrag – 8 a § andra stycket

Enligt 8 a § andra stycket ska den som begär ett utdrag om sig själv ur misstankeregistret, på samma sätt som när utdrag begärs ur belastningsregistret, göra det genom en skriftlig begäran som undertecknas av den sökande. Som vi anför när det gäller belastningsregistret finns skäl att förändra kravet i enlighet med de förslag och överväganden Utredningen om 2016 års dataskyddsdirektiv har gjort.¹² Vi föreslår alltså samma ändring i lagen om misstankeregister. För en utförligare redogörelse, se avsnitt 5.5.

Skadestånd och rättelse – 15 §

Som vi anför i våra allmänna överväganden (avsnitt 2.6.7) behövs inte någon hänvisning till bestämmelser om rättelse m.m i brottsdatalagen för att dessa bestämmelser ska kunna tillämpas i stället för regleringen i personuppgiftslagen när denna lag upphävs. En hänvisning behövs däremot till 7 kap. 1 § brottsdatalagen om skadestånd. En sådan hänvisning bör införas och utformas i enlighet med motsvarande bestämmelser i 20 § lagen om belastningsregister, se vidare våra överväganden i avsnitt 5.5.

Det kan anmärkas att frågor om radering ur registret skulle kunna aktualiseras om ett avsnitt i registret är helt och hållet felaktigt, exempelvis med anledning av en personförväxling. Sådan radering är möjlig med stöd av 4 kap. 9 § brottsdatalagen, eftersom raderingen i det fallet är det relevanta sättet att rätta personuppgiften.¹³ Någon hänvisning till brottsdatalagen behövs inte för att den enskilde ska kunna begära rättelse i det avseendet.

Som vi tidigare redogjort för kommer dataskyddsförordningen att vara tillämplig på vissa behandlingar som avser utlämnande ur registret. Som vi också anför anser vi att förändret av registret dock faller under det nya dataskyddsdirektivets, och därmed brottsdatalagens, tillämpningsområde. Eftersom personuppgifternas korrekthet har att göra med vad som en gång förs in i registret kommer frågor om rättelse m.m. inte att bedömas enligt

¹² SOU 2017:29 s. 413–415.

¹³ Se vidare SOU 2017:29 s. 405.

dataskyddsförordningen. Detta gäller även om en eventuell felaktighet i registret skulle uppmärksammas i samband med ett utlämnande som i och för sig omfattas av förordningens tillämpningsområde.

Sanktionsavgifter

Som vi redogör för i våra allmänna överväganden (avsnitt 2.6.7) anser vi att det inte behöver införas särskilda bestämmelser om sanktionsavgifter i registerförfattningar som ingår i vårt uppdrag och som omfattas av det nya dataskyddsdirektivets tillämpningsområde. Inte heller i förhållande till dataskyddsförordningen behövs bestämmelser om sanktioner, se vidare avsnitt 2.5.9.

Bör gallringsbestämmelserna omformuleras?

Som vi redogjort för i avsnitt 5.5 anser Utredningen om 2016 års dataskyddsdirektiv att det är motiverat att i vissa registerförfattningar som omfattas av det nya dataskyddsdirektivets område renodla terminologin när det gäller gallring och längsta tid för behandling av personuppgifter. Vi har i det avsnittet kommit fram till att vi inte anser att det finns skäl att förändra bestämmelser om gallring i lagen om belastningsregister. Vi gör samma bedömning när det gäller lagen om misstankeregister. Våra överväganden framgår av avsnitt 5.5.

Behövs bestämmelser som inskränker den enskildes rättigheter?

Som vi anført i våra allmänna överväganden (avsnitt 2.6.6) finns ingen anledning för oss att överväga inskränkningar i den registrerades rättigheter enligt det nya dataskyddsdirektivet.

Även om vissa utlämnanden ur misstankeregistret ska bedömas enligt dataskyddsförordningen blir det, som anförts ovan, inte aktuellt att tillämpa vissa bestämmelser i förordningen, eftersom själva insamlandet av personuppgifter till registret och bevarandet i registret regleras av det nya dataskyddsdirektivet. Frågor om information, rättelse och radering, som i förordningen regleras i

artiklarna 13–17, regleras därmed av brottsdatalagen. Teoretiskt kan man dock tänka sig en tillämpning av rätten till begränsning av behandling och rätten att göra invändningar mot behandling, eftersom den enskilde skulle kunna vända sig emot just ett visst, eller en viss typ av utlämnande, för ett sådant ändamål som inte omfattas av det nya dataskyddsdirektivet och därmed regleras av dataskyddsförordningen. Samtidigt är det svårt att föreställa sig att det någonsin skulle kunna bli fråga om att faktiskt begränsa behandlingen i enlighet med artikel 18 eller artikel 21. Eftersom utlämnanden är författningsreglerade, liksom alla de olika tillstånds- eller lämplighetsprövningar i vilka uppgifter ur misstankeregistret kan behövas, måste det i praktiken bli nära nog omöjligt för den enskilde att åberopa några relevanta skäl. Det torde i de allra flesta fall vara tillräckligt för Polismyndigheten att hänvisa till författningsregleringen för att bemöta eventuella invändningar eller en begäran om begränsning, jfr vad vi anfört i våra allmänna överväganden. Vi anser därmed att det inte finns skäl att införa några bestämmelser i författningarna som rör inskränkningar i den registrerades rättigheter enligt dataskyddsförordningen.

Slutligen ska anmärkas att om den registrerade begär rättelse av uppgifterna i registret i enlighet med 4 kap. 9 § brottsdatalagen och det inte genast går att fastställa om uppgifterna är korrekta eller inte, har Polismyndigheten en skyldighet enligt paragrafens andra stycke att begränsa behandlingen. En sådan begränsning torde omfatta utlämnanden eller annan vidarebehandling som i och för sig inte omfattas av brottsdatalagens tillämpningsområde. I vart fall kommer tekniska åtgärder för att begränsa behandlingen av praktiska skäl troligen att omfatta all vidare behandling, oavsett vilket regelverk som skulle varit tillämpligt på behandlingen om den utförts.

7 Lagen och förordningen om Schengens informationssystem

7.1 Om författningarna

Bakgrund

I syfte att påskynda förverkligandet av den fria rörligheten för personer ingick Frankrike, Tyskland och Beneluxstaterna år 1985 ett avtal om att successivt avveckla personkontrollerna vid de gemensamma gränserna och att utveckla det polisiära och rättsliga samarbetet mellan staterna. Avtalet, som var ett separat mellanstatligt avtal utanför EU, ingicks i gränsorten Schengen i Luxemburg och går därför under benämningen Schengenavtalet. Efter hand har fler av EU:s medlemsstater anslutit sig till avtalet. Sverige gjorde det 1996.¹

De viktigaste reglerna för samarbetet, bl.a. de praktiska åtgärderna för att genomföra avvecklingen av personkontrollerna vid de inre gränserna, fanns ursprungligen i Schengenkonventionen, som började tillämpas 1995. I samband med Amsterdamfördragets ikraftträdande den 1 maj 1999 införlivades Schengenregelverket i EU-rätten. Detta innebär att samarbetet numera äger rum i den vanliga EU-strukturen, dvs. under medverkan av EU:s institutioner. Regelverket omfattar olika EU-rättsakter som utvecklar bestämmelserna i det ursprungliga Schengenavtalet och –konventionen. När det gäller Schengens informationssystem (SIS) har reglerna om detta i Schengenkonventionen ersatts av EU-rättsakter, ett rådsbeslut och två förordningar. Rådets beslut 2007/533/RIF av den 12 juni 2007 om inrättande, drift och användning av andra generationen av Schengens informations-

¹ Prop 2009/10:86 s. 19.

system (SIS II) (kallas *rådsbeslutet* i det följande) är en reglering som faller inom den tidigare s.k. pelarstrukturen, som gällde för EU-samarbetet innan Lissabonfördraget trädde i kraft. Rådsbeslutet avser tredjepelarfrågor – polisiärt och straffrättsligt samarbete mellan EU:s medlemsstater. Före Lissabonfördraget hade detta samarbete mellanstatlig karaktär.²

Utöver rådsbeslutet regleras alltså användningen av SIS av två EU-förordningar. Den ena avser vad som tidigare var s.k. förstapelarfrågor, dvs. gränskontroll och immigrationskontroll. Den andra förordningen avser tillgång till SIS för de enheter inom medlemsstaterna som ansvarar för att utfärda registreringsbevis för fordon.³

SIS är ett datasystem som används för informationsutbyte mellan medlemsstaterna emellan. Det är bl.a. ett hjälpmedel för efterlysning och spaning och innehåller uppgifter om personer och om föremål som är efterlysta eller på annat sätt eftersökta.⁴

Kommissionens förslag till nya EU-rättsakter om SIS

Andra generationen av Schengens informationssystem (SIS II) togs i bruk den 9 april 2013. Under år 2016 har kommissionen genomfört en utvärdering av systemet och informationsutbytet ur olika aspekter. I sin utvärderingsrapport drar kommissionen slutsatsen att systemet är en framgång och att det fungerar mycket väl. Samtidigt pekar man på behov och möjligheter att förbättra det ytterligare. Kommissionen har lagt fram förslag till tre nya förordningar avseende SIS. Anledningen till uppdelningen är att förslagen bygger på skilda EU-rättsliga grunder. En förordning kommer att avse användningen av SIS för gränskontroll, en kommer att behandla brottsbekämpning etc., och en kommer att avse kontroll av återvändandebeslut. Den sista användningen av SIS

² A. prop. s. 18 och 21 f.

³ Förordningarnas fullständiga namn är Europaparlamentets och rådets förordning (EG) nr 1987/2006 av den 20 december 2006 om inrättande, drift och användning av andra generationen av Schengens informationssystem (SIS II) respektive Europaparlamentets och rådets förordning (EG) nr 1986/2006 av den 20 december 2006 om tillträde till andra generationen av Schengens informationssystem (SIS II) för de enheter i medlemsstaterna som ansvarar för att utfärda registreringsbevis för fordon, se vidare prop. 2009/10:86.

⁴ A. prop. s 20.

är en nyhet. Kommissionens utvärderingsrapport och förslag till nya förordningar lades fram i december 2016.⁵

Kort om innehållet i lagen och förordningen om SIS

Lagen (2000:344) och förordningen (2000:836) om Schengens informationssystem (kallas *lagen* respektive *förordningen om SIS* i det följande) genomförde först Schengenkonventionen, sedan det ovan nämnda rådsbeslutet om SIS II, i svensk rätt.⁶ Schengenkonventionen, och följaktigen lagen om SIS, reglerade från början hela användningen av SIS. När regleringen på EU-nivå delades upp i två förordningar och ett rådsbeslut medförde detta att vissa bestämmelser i lagen om SIS, som avsåg användningen av SIS inom förordningarnas tillämpningsområde, fick tas bort. Den svenska förordningen om SIS innehåller dock alltjämt en bestämmelse om tillgång till SIS för myndigheter som prövar ansökningar om visering och upphållstillstånd (9 §). I lagen om SIS finns också upplysande bestämmelser om regleringen i EU-förordningarna m.m. (se 9 § andra, tredje och fjärde styckena).

Lagen ålägger Polismyndigheten att med hjälp av automatiserad behandling föra det register som är den svenska nationella enheten av SIS (1 §). Lagen innehåller vidare ändamålen med registret, vilka uppgifter som får registreras och andra förutsättningar för att registrering ska få ske (2–7 §§). Lagen innehåller också bestämmelser om vilka myndigheter som kan få ut uppgifter ur registret, hur uppgifterna får användas och vad som gäller för gallring av uppgifterna (9–11 §§). Bestämmelser om s.k. tilläggsinformation finns i 12–14 §§. Tilläggsinformation registreras inte i SIS, men utbyts mellan Schengenstaterna, bl.a. efter att en sökning i systemet har lett till en träff. Tilläggsinformation får endast användas för att uppnå det syfte för vilket den har överlämnats och

⁵ En översiktlig presentation av kommissionens förslag m.m. finns i regeringskansliets faktapromemoria 2016/17:FPM58. Originaldokumenten från kommissionen har beteckningarna COM(2016) 880 (utvärderingsrapporten) samt COM(2016) 881, 882 och 883 (förslag till förordningar).

⁶ Lagen genomförde alltså från början Schengenkonventionens reglering av SIS (prop. 1999/2000:64). Lagändringar som krävdes för att genomföra det senare antagna rådsbeslutet och trädde i kraft 2013 (SFS 2010:380, prop. 2009/10:86.)

får inte bevaras längre än vad som behövs för att uppnå det syfte för vilket den har mottagits.

Slutligen innehåller lagen bestämmelser om rättelse, skadestånd och överklagande (15–17 §§).

När det gäller sekretess för uppgifterna i registret finns en särskild sekretessbestämmelse i 37 kap. 6 § offentlighets- och sekretesslagen (2009:400). Avsikten med den särskilda sekretessbestämmelsen är att garantera sekretess för uppgifter som i förekommande fall inte omfattas av sekretess enligt andra bestämmelser.⁷ Lagen om SIS innehåller en upplysning om sekretessen i 8 § som hänvisar till offentlighets- och sekretesslagen.

Förordningen om SIS innehåller bestämmelser som rör informations- och uppgiftsskyldighet för Polismyndigheten i olika situationer. I förordningen finns också bestämmelser om hur information om behandlingen i systemet ska registreras (loggningsuppgifter) och en skyldighet att föra statistik över vissa beslut. I förordningen har tagits in en bestämmelse som hänvisar till personuppgiftslagens bestämmelser om information till den som registrerats (21 §).

7.2 Vilken EU-rättsakt är tillämplig?

Bedömning: Personuppgiftsbehandlingen i SIS omfattas antingen av det nya dataskyddsdirektivets tillämpningsområde eller av dataskyddsförordningens. Syftet med behandlingen är avgörande för vilken rättsakt som är tillämplig.

Skälen för bedömningen: SIS är ett datasystem som innehåller personuppgifter. Behandlingen av personuppgifter i SIS är alltså en sådan behandling som regleras av antingen det nya dataskyddsdirektivet eller dataskyddsförordningen.

Som tidigare nämnts inordnas rådsbeslutet under området polis-samarbete och straffrättsligt samarbete. Numera regleras sådana frågor i kapitel 4 och 5 i fördraget om Europeiska unionens funktionssätt. Kommissionens förslag till förordning som gäller

⁷ A. prop. s. 25. Se även prop. 1999/2000:64 s. 144 f.

brottsbekämpning m.m. har artiklar i dessa kapitel som rättslig grund.⁸ Att SIS i denna del avser polis- och straffrättsligt samarbete innebär inte i sig att personuppgiftsbehandlingen inom ramen för detta samarbete omfattas av det nya dataskyddsdirektivets tillämpningsområde. Detta framgår tydligt av kommissionens förslag, som anger att dataskyddsförordningen ska tillämpas på personuppgiftsbehandlingen, utom såvitt avser personuppgiftsbehandling som omfattas av det nya dataskyddsdirektivets tillämpningsområde. I sådana fall ska den nationella rätt som genomför direktivet tillämpas (artikel 64). Av förslaget framgår att det omfattar en rätt till åtkomst för vissa myndigheter som i normalfallet inte kan anses vara brottsbekämpande i det nya dataskyddsdirektivets mening (artikel 44 och 45). Kommissionens förslag innehåller dock ingen precisering av om det är detta förhållande som gör dataskyddsförordningen tillämplig, eller om det finns även annan personuppgiftsbehandling i SIS som omfattas av dataskyddsförordningen.

Regeringen anförde vid genomförandet av Schengenkonventionen att mycket av informationsutbytet inom SIS skulle komma att avse underrättelseverksamhet och utredning om brott. Dock skulle visst informationsutbyte kunna ske för "helt andra syften", exempelvis uppgifter om försvunna personer som ska omhändertas för sin egen säkerhet.⁹ Av 5 § i förordningen om SIS följer att framställningar om sådana försvunna personer för svenskt vidkommande kan avse personer som tvångsvårdas av olika anledningar, exempelvis unga och missbrukare. Datainspektionen har i ett beslut som återges i vårt kapitel om efterlysningskungörelsen (avsnitt 13) uttalat att behandling av information om personer som tvångsvårdas inte kan inordnas under polisdatalagens (2010:361) tillämpningsområde. Datainspektionen ansåg att sådan personuppgiftsbehandling inte kan anses ske inom ramen för brottsbekämpande verksamhet.

Sammanfattningsvis gör vi bedömningen att utgångspunkten för analysen av lagen och förordningen om SIS får vara att en registrering i SIS och den fortsatta behandlingen av personuppgifterna i systemet kan omfattas antingen av det nya dataskydds-

⁸ Framgår av förslaget (COM [2016] 883 final eller se regeringskansliets faktabromemoria 2016/17:FPM58 s. 6.

⁹ Prop 1999/2000:64 s. 149 f.

direktivets *eller* dataskyddsförordningens tillämpningsområde, beroende på syftet med registreringen. Skulle detta ställnings-tagande omprövas kan våra förslag justeras därefter. Det skulle i så fall innebära att all förekommande personuppgiftsbehandling i SIS ska anses omfattas av det nya dataskyddsdirektivets tillämpningsområde. Våra författningsförslag kan i princip användas även för detta fall, med den ändringen att den upplysande bestämmelsen om dataskyddsförordningen och dataskyddslagen får utgå.

7.3 Överväganden om befintliga bestämmelser

7.3.1 Överväganden i förhållande till det nya dataskyddsdirektivet

Bedömning: Författningsregleringen är i huvudsak förenlig med det nya dataskyddsdirektivet. Hänvisningar till personuppgiftslagen innebär att 16 § i lagen och 21 § i förordningen måste ändras.

Skälen för bedömningen:

Den svenska regleringen är i huvudsak förenlig med direktivet

Det nya dataskyddsdirektivet innehåller en uttrycklig reglering av förhållandet till tidigare EU-rättsakter i artikel 60. Enligt artikeln ska tidigare bestämmelser om dataskydd i rättsakter inom området för polisiärt och straffrättsligt samarbete inte påverkas av det nya direktivet. Som vi diskuterar i våra allmänna överväganden, avsnitt 2.6.3, är det i viss mån tveksamt vilka bestämmelser i tidigare EU-rättsakter som artikeln är tillämplig på. Eftersom stora delar av regleringen i lagen och förordningen om SIS under alla förhållanden är förenlig med direktivet behöver dock artikel 60 inte tillämpas för att behålla den svenska regleringen. Det gäller följande paragrafer i lagen

- 1 § (den grundläggande bestämmelsen om den svenska enheten av SIS och Polismyndighetens personuppgiftsansvar)
- 2 § (ändamålet med SIS)

- 3–6 §§ (uppgifter som SIS får innehålla och förutsättningar för att föra in information i systemet)
- 8 § (upplyser om regleringen i sekretesslagen)
- 9 § (svenska myndigheter som har rätt att få tillgång till registret)
- 11 och 14 §§ (gallring)
- 12 § (definitionen av s.k. tilläggsinformation).

I 5 § hänvisas till personuppgiftslagen och till polisdatalagen. Paragrafen måste alltså ändras eftersom personuppgiftslagen upphävs och polisdatalagen får ett nytt namn. Utredningen om 2016 års dataskyddsdirektiv föreslår dessa ändringar och att hänvisningen till personuppgiftslagen ersätts av en hänvisning till brottsdatalagen. Vi återkommer i avsnitt 7.3.2 till frågan om 5 § behöver ändras som en följd av att dataskyddsförordningen får anses tillämplig på viss behandling i SIS.¹⁰

Den svenska författningsregleringen av SIS kan anses utgöra en rättslig grund för behandlingen som gör den tillåten enligt det nya dataskyddsdirektivet och enligt brottsdatalagen.¹¹ De bestämmelser som anges ovan är vidare sådana preciseringar och begränsningar av personuppgiftsbehandlingen som är förenliga med direktivet (se vidare våra allmänna överväganden i avsnitt 2.6.1 och 2.6.3). Förordningen innehåller i stora delar fortsatta preciseringar av lagregleringen samt reglering av vissa frågor om informations-skyldighet och s.k. flaggning som följer av rådsbeslutet och som under alla förhållanden måste anses förenlig med dataskyddsdirektivet. I 21 § i förordningen finns dock hänvisningar till personuppgiftslagen och paragrafen måste därför ändras redan av det skälet. Våra överväganden följer i avsnitt 7.4.

Att reglera möjligheten till skadestånd är i sig förenligt med direktivet (jfr 7 kap. 1 § brottsdatalagen). Bestämmelsen i 16 §

¹⁰ Utredningen om 2016 års dataskyddsdirektiv föreslår en ändring till följd av att personuppgiftslagen upphör att gälla och polisdatalagen byter namn, se SOU 2017:74 s. 74.

¹¹ Dock kan inte enbart regleringen i SIS åberopas som rättslig grund för att föra in uppgifter där, utan det ska också, vilket framgår av 5 §, finnas stöd i annan svensk författning. Se vidare prop. 1999/2000:64 s. 134.

måste dock även den ändras som en följd av att personuppgiftslagen upphävs.

Enligt 4 § i lagen om SIS är det tillåtet att föra in uppgifter om fingeravtryck i SIS. Biometriska uppgifter (och vissa andra särskilda kategorier av personuppgifter) regleras i artikel 10 i det nya dataskyddsdirektivet.¹² När det gäller biometriska uppgifter har artikeln genomförts i 2 kap. 12 § brottsdatalagen. Enligt bestämmelsen får biometriska uppgifter endast behandlas om det är absolut nödvändigt för ändamålet med behandlingen och om det är särskilt föreskrivet. Behandlingen av fingeravtryck i SIS får anses förenlig både med brottsdatalagen och med det nya dataskyddsdirektivet.

När det gäller det absoluta förbudet att behandla vissa andra känsliga personuppgifter i SIS (7 §) är det också förenligt med det nya dataskyddsdirektivet, eftersom möjligheten att behandla känsliga personuppgifter ska avgöras i nationell rätt (artikel 10). Vi återkommer i avsnitt 7.4 till hur 7 § SIS förhåller sig till 2 kap. 11 § brottsdatalagen.

Användningsbegränsningar

Artikel 60 får, enligt vår mening, en praktisk betydelse först när det gäller vissa bestämmelser som helt eller delvis avviker från regleringen i det nya dataskyddsdirektivet.

Rådsbeslutet innehåller några bestämmelser som innebär en inskränkning av behandlingsmöjligheterna i SIS jämfört med vad som är tillåtet enligt det nya dataskyddsdirektivet. Bestämmelserna har genomförts i 10 och 13 §§ lagen om SIS som avser dels begränsningar av viss vidarebehandling med avseende på ändamålen för behandling, dels ett förbud mot att överföra uppgifter i SIS till tredje land och internationella organisationer. Det nya dataskyddsdirektivet tillåter både vidarebehandling för nya ändamål inom direktivets tillämpningsområde och överföringar till tredje land och internationella organisationer, dock under vissa förutsättningar. Redan av detta kan anses följa att det finns möjlighet att på nationell nivå avgöra att några sådana förutsättningar inte föreligger

¹² Fingeravtryck är alltså en biometrisk uppgift, se definitionen av uttrycket i 1 kap. 6 § och vidare SOU 2917:29 s. 266.

och att därmed begränsa behandlingsmöjligheterna i nationell rätt. Inskränkningarna i behandlingsmöjligheterna kan därtill betraktas som åtgärder som ger ett starkare skydd för den enskildes integritet. Starkare skyddsåtgärder är förenliga med dataskyddsdirektivet i enlighet med artikel 1.3. Till detta kommer att användningsbegränsningar som följer av tidigare EU-rättsakter torde vara förenliga med direktivet med en tillämpning av artikel 60.¹³

Rättelse och radering

Rådsbeslutet innehåller artiklar som avser rättelse och radering av personuppgifter som har genomförts i 15 § lagen om SIS. Den enskildes rätt att begära åtgärderna följer av artikel 58.5 i rådsbeslutet. En orsak till att en särskild bestämmelse om rättelse m.m. ansågs vara nödvändig i lagen om SIS var att personuppgiftslagens reglering endast gäller i förhållande till personuppgiftsbehandling enligt den lagen. Den svenska regleringen i lagen om SIS tar upp åtgärden *blockering* trots att blockering inte nämns i rådsbeslutet. Det utvecklades inte i de svenska förarbetena när blockering skulle kunna komma i fråga eller på vilket sätt en blockering i SIS rent praktiskt skulle utföras.

Bestämmelserna i rådsbeslutet om rättelse och radering får anses vara sådana dataskyddsbestämmelser som i och för sig inte ska påverkas av det nya dataskyddsdirektivet i enlighet med artikel 60. Med beaktande enbart av direktivets reglering skulle man alltså kunna ha kvar den svenska lagregleringen som den är. Det finns då heller inget hinder emot att behålla bestämmelsen i 17 §, som avser överklagande av beslut enligt 15 §. Ordalydelsen i 15 § skulle dock behöva ändras under alla förhållanden, eftersom uttrycken *utplåning* och *blockering* inte längre kommer att användas i dataskyddsrättsliga sammanhang efter det att personuppgiftslagen upphört att gälla.

Samtidigt kan man konstatera att det som kommer att gälla enligt brottsdatalagen ifråga om rättelse och radering inte kan anses skilja sig i sak från vad rådsbeslutet kräver i fråga om dessa åtgärder. Skyldigheten att rätta felaktiga personuppgifter följer av 4

¹³ SOU 2017:29 s. 290 f.

kap. 9 § brottsdatalagen. Enligt 4 kap. 10 § ska personuppgifter raderas om de behandlas i strid med lagens krav på personuppgiftsbehandling, bl.a. i fråga om rättslig grund för behandlingen (2 kap. 1 §). Denna skyldighet får anses motsvara skyldigheten enligt rådsbeslutet att radera ”olagligt lagrade” personuppgifter. Vi gör fortsatta överväganden om behovet av att ändra eller upphäva 15 § lagen om SIS i avsnitt 7.4.

Information till den registrerade

I 21 § i förordningen finns hänvisningar till personuppgiftslagen som alltså behöver ändras I övrigt innehåller bestämmelsen vissa tidsgränser för att lämna informationen, som bl.a. följer av artikel 58.6 i rådsbeslutet (senast 60 dagar efter begäran). Enligt det nya dataskyddsdirektivet fastställs ingen sådan exakt tidsgräns för att lämna information efter begäran. Enligt 4 kap. 3 § brottsdatalagen ska den personuppgiftsansvarige lämna information utan onödigt dröjsmål. Eftersom tidsfristerna följer av en sådan tidigare EU-rättsakt som avses i artikel 60 påverkas regleringen i den delen inte av direktivet redan av den anledningen.

7.3.2 Överväganden i förhållande till dataskyddsförordningen

Bedömning: Regleringen i lagen och förordningen om SIS är i huvudsak förenlig med dataskyddsförordningen. Bestämmelserna om rättelse och radering (15 §) och överklagande av sådana beslut (17 §) bör dock inte vara tillämpliga på personuppgiftsbehandling inom dataskyddsförordningens tillämpningsområde. Bestämmelser som hänvisar till personuppgiftslagen måste ändras redan som en följd av att personuppgiftslagen kommer att upphävas.

Regleringen är i huvudsak förenlig med dataskyddsförordningen

Beroende på innehållet och syftet med en registrering i SIS kan alltså dataskyddsförordningen vara tillämplig på behandlingen av personuppgifter i SIS.

Medlemsstaterna är rättsligt förpliktade genom rådsbeslutet att upprätta den nationella delen av SIS (*N.SIS*). Personuppgiftsbehandlingen i SIS kan därmed sägas ha en rättslig förpliktelse som grund (artikel 6.1 c). Varje medlemsstat förfogar dock över möjligheten att föra in uppgifter i SIS. Användningen av SIS (även för syften som ligger utanför det nya dataskyddsdirektivets tillämpningsområde) får även anses ingå i ett uppdrag av allmänintresse.¹⁴ Vidare är införande i SIS beroende av att behandling av motsvarande slag av uppgifter är tillåten enligt personuppgiftslagen, polisdatalagen eller annan svensk författning, vilket framgår av 5 §. Kravet på rättslig grund enligt dataskyddsförordningens artikel 6.3 får alltså anses uppfyllt både på unionsnivå och på nationell nivå, genom författningsregleringen av SIS och annan tillämplig författningsreglering.

När det gäller 5 § i lagen måste den dock ändras som en följd av att personuppgiftslagen upphör att gälla. Som Utredningen om 2016 års dataskyddsdirektiv föreslår bör den nuvarande hänvisningen till personuppgiftslagen tas bort. Utredningen föreslår att den ersätts av en hänvisning till brottsdatalagen. När det gäller behandling inom dataskyddsförordningens tillämpningsområde behövs ingen annan ändring av 5 §, eftersom bestämmelsen också hänvisar till ”annan svensk författning”. Den rättsliga grund för personuppgiftsbehandling som krävs enligt dataskyddsförordningen måste vara fastställd enligt nationell rätt. Det är alltså inte lämpligt att föra in någon hänvisning till dataskyddsförordningen i 5 §, eftersom dataskyddsförordningen i sig inte kan utgöra en rättslig grund för personuppgiftsbehandling som sker med stöd av ett uppdrag av allmänt intresse i enlighet med 6.1 e. Eftersom Utredningen om 2016 års dataskyddsdirektiv föreslagit den ändring som behövs i 5 § lämnar vi inget sådant författningsförslag.¹⁵

Regleringen utgör i övrigt sådana preciseringar av personuppgiftsbehandlingen som är tillåtna enligt förordningens artikel 6.2. Vi anser alltså att 1–5, 8, 9, 11, 12 och 14 §§ är förenliga med dataskyddsförordningen, liksom bestämmelserna i förordningen om SIS. När det gäller bestämmelserna om gallring (11 och 14 §§)

¹⁴ Polismyndigheten har enligt efterlysningkungörelsen i uppdrag att efterlysa och föra register över personer som eftersöks. Det kan gälla personer som tvångsvårdas av olika anledningar, se vidare kap. 13.

¹⁵ Se SOU 2017:74 s. 74

avser de delvis vad som får betraktas som en upprepning av principen om lagringsminimering i artikel 5.1 e. Eftersom paragraferna också har ett vidare innehåll, där mer specifika tidsgränser för lagring slås fast, menar vi att de bör kunna behållas i sin helhet för att ge en mer sammanhängande och förståelig reglering i enlighet med skäl 8. Av betydelse för den bedömningen är också att bestämmelserna samtidigt reglerar bevarande och gallring inom det nya dataskyddsdirektivets tillämpningsområde och att en uppdelning av regleringen skulle göra den onödigt komplex.

Användningsbegränsningar och känsliga personuppgifter¹⁶

Som vi redogjort för i våra allmänna överväganden finns det inget i dataskyddsförordningen som hindrar en begränsning av myndigheters behandlingsmöjligheter. Att inskränka möjligheten att vidarebehandla personuppgifter är därmed förenligt med förordningen. De bestämmelser som begränsar vidarebehandling i 10 och 13 §§ kan därför behållas. Detsamma gäller bestämmelsen i 10 § som förbjuder överföringar till tredje land och internationella organisationer.

När det gäller känsliga personuppgifter är utgångspunkten i dataskyddsförordningen att det är förbjudet att behandla sådana uppgifter. Bestämmelsen i 7 § överensstämmer alltså med artikel 9 såvitt avser de kategorier av personuppgifter som tas upp i bestämmelsen. Samtidigt är det tillåtet att behandla fingeravtryck i SIS (en biometrisk uppgift). Denna behandling följer av rådsbeslutet och har därmed en grund i unionsrätten samt måste anses nödvändig av hänsyn till ett viktigt allmänt intresse (artikel 9.2 g). Regleringen av känsliga personuppgifter i 7 § och 4 § 3 i lagen om SIS utgör därmed en tillåten författningsreglering i förhållande till dataskyddsförordningen.

¹⁶ Det kan noteras att SIS, i motsats till de flesta andra register, inte innehåller personnummer utan endast födelsedatum, se 4 § första stycket 4.

Rättelse, radering och överklagande

Dataskyddsförordningen innehåller rättigheter för den enskilde att få ofullständiga och oriktiga personuppgifter rättade och raderade. Vidare innehåller förordningen rättigheter när det gäller s.k. begränsning av behandlingen av personuppgifter (se vidare våra allmänna utgångspunkter, avsnitt 2.5.8).

Rådsbeslutet anger att den enskilde ska ha rätt att få oriktiga uppgifter rättade och olagligt lagrade uppgifter raderade. Rådsbeslutet i denna del har genomförts i 15 § lagen om SIS, som dock även medför en rätt till *blockering*.

Till skillnad från det nya dataskyddsdirektivet innehåller dataskyddsförordningen inte någon bestämmelse om förhållandet till tidigare EU-rättsakter. Frågan är då om regleringen i 15 § lagen om SIS innebär en avvikelse från förordningens reglering (och om denna avvikelse i så fall är tillåten enligt artikel 23 i förordningen) eller om regleringen i sak överensstämmer med förordningens bestämmelser. Det sistnämnda skulle innebära att den svenska lagregleringen bör utgå, eftersom förordningen ska tillämpas direkt.

Dataskyddsförordningen innehåller en rätt för den enskilde att begära rättelse av oriktiga personuppgifter (artikel 16). I det avseendet är det alltså ingen skillnad mellan 15 § i lagen om SIS (eller det bakomliggande rådsbeslutet) och dataskyddsförordningen. Rätten till radering i artikel 17 i dataskyddsförordningen, artikel 17.1 och 17.2, gäller inte om personuppgiftsbehandlingen är nödvändig för att utföra en rättslig förpliktelse eller utföra en uppgift av allmänt intresse, dvs. sådan personuppgiftsbehandling som har en rättslig grund i enlighet med artikel 6.1 c eller e (artikel 17.3). Om en personuppgiftsansvarig behandlar personuppgifter på ett olagligt sätt, dvs. utför en behandling utöver de förutsättningar som gäller enligt den tillämpliga rättsliga grunden, torde det innebära att undantaget från rätten till radering inte är tillämpligt. Under alla förhållanden följer det av de allmänna principerna för personuppgiftsbehandling att olaglig behandling måste upphöra. Om sådan olaglig behandling utgörs av registrering i ett visst datasystem, som SIS, måste följden i normalfallet vara att uppgifterna raderas ur datasystemet.

Vi menar alltså att dataskyddsförordningen i sak överensstämmer med rådsbeslutets krav. Dataskyddsförordningen bör därför tillämpas direkt såvitt avser rättelse och radering. Bestämmelsen om överklagande (17 §) blir därmed inte aktuell att tillämpa inom dataskyddsförordningens tillämpningsområde. Vi överväger hur bestämmelserna lämpligen bör ändras i avsnitt 7.4.

Skadestånd

Som vi redan anfört i våra generella överväganden menar vi att det på dataskyddsförordningens område inte längre behövs några bestämmelser om skadestånd utöver den generella bestämmelse som Dataskyddsutredningen föreslagit i 8 kap. 1 § dataskyddslagen. Den bestämmelse som f.n. finns i 16 § lagen om SIS måste ändras till följd av att personuppgiftslagen upphör att gälla. Vi återkommer i nästa avsnitt med förslag till ändringar i bestämmelsen som tar hänsyn både till det nya dataskyddsdirektivet och dataskyddsförordningen.

7.3.3 Genomförandet av rådsbeslutet när personuppgiftslagen upphävs

Bedömning: För att rådsbeslutet ska vara korrekt genomfört även efter det att personuppgiftslagen upphävts, behövs reglering som gäller utöver lagen och förordningen om SIS. Rådsbeslutet blir korrekt genomfört om lagen om SIS gäller utöver brottsdatalagen respektive kompletterar dataskyddsförordningen.

Skälen för bedömningen:

Genomförande av rådsbeslutet förutsätter kompletterande bestämmelser

Rådsbeslutet genomfördes i svensk rätt dels av lagen och förordningen om SIS, dels genom regleringen i personuppgiftslagen. Vissa artiklar i rådsbeslutet ansågs alltså inte kräva några lagstiftnings-

åtgärder med hänvisning till personuppgiftslagens redan gällande bestämmelser. När det gällde datasäkerhet (artikel 10), loggning (artikel 12), personalutbildning (artikel 14), datakvalitet (artikel 49) och tillämpning av Europarådets konvention om skydd vid automatisk databehandling av personuppgifter (artikel 57) ansågs personuppgiftslagens reglering redan genomföra kraven i rådsbeslutet. Särskilt hänvisades till 9 och 31 §§. Vidare anfördes mer generellt att personuppgiftslagens reglering inte borde frångås i någon del.¹⁷ Det kan anmärkas att artikel 46.9 i rådsbeslutet anger att i den mån inga särskilda bestämmelser föreskrivs i EU:s lagstiftning ska varje medlemsstats nationella lagstiftning gälla för de uppgifter som läggs in i den nationella enheten av SIS (*N.SIS*).

För att rådsbeslutet även fortsättningsvis ska anses korrekt genomfört i svensk rätt krävs alltså att det i stället för personuppgiftslagen finns en generell reglering som kan anses genomföra kraven i de nämnda artiklarna i rådsbeslutet. På den personuppgiftsbehandling som omfattas av dataskyddsförordningens tillämpningsområde är det självklart att dataskyddsförordningen också utgör den övergripande regleringen på området. När det gäller personuppgiftsbehandling inom det nya dataskyddsdirektivets tillämpningsområde måste det i stället bli den nationella lagstiftning som genomför direktivet som blir tillämplig, dvs. brottsdatalagen. Det kan anmärkas att artikel 60 visserligen ger tidigare EU-rättsakter företräde om de innehåller avvikande bestämmelser om dataskydd. Bestämmelsen kan dock inte vara ett hinder emot att tillämpa nationell lagstiftning som genomför direktivet, även inom tillämpningsområdet för tidigare EU-rättsakter, så länge de tidigare EU-rättsakterna blir korrekt genomförda.

En konsekvens av att personuppgiftslagen upphävs är vidare, liksom för flertalet andra författningar avseende personuppgiftsbehandling, att bestämmelser med hänvisningar till den lagen måste ändras eller upphävas. Det gäller 5 och 16 §§ i lagen om SIS och 21 § i förordningen. Vi återkommer till detta i våra förslag till författningsändringar i nästa avsnitt.

¹⁷ Prop. 2009/10:86 s. 25 f., 40 och 45 f.

Datakvalitet (artikel 49)

Enligt artikel 49.1 ansvarar varje medlemsstat för att uppgifter som läggs in i SIS är korrekta, aktuella och läggs in i SIS lagligen. Det är endast den medlemsstat som lagt in uppgifter i SIS som har befogenhet att företa någon åtgärd, exempelvis radera eller korrigera, uppgifterna. I artikelns följande delar regleras hur medlemsstaterna ska agera om någon annan medlemsstat än den som lagt in uppgifter har fått kännedom om felaktigheter i en registrering.

Regeringen anförde att med personuppgiftsansvaret (som då föll på Rikspolisstyrelsen, i dag på Polismyndigheten) följde de skyldigheter som framgår av 9 § personuppgiftslagen, innefattande bl.a. skyldigheten att se till att alla rimliga åtgärder vidtas för att rätta, blockera och utplåna felaktiga personuppgifter (9 § h). Några lagstiftningsåtgärder krävdes därmed inte för att genomföra artikel 49. Rådsbeslutets bestämmelser om förfarandet medlemsstaterna emellan vid misstänkta felaktigheter i registret reglerades i förordningen (17 §).¹⁸

Brottsdatalagens grundläggande krav på behandling av personuppgifter innefattar att de ska behandlas författningsenligt (2 kap. 6 §), att de ska vara korrekta och uppdaterade, om nödvändigt, och att alla rimliga åtgärder ska vidtas för att personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålen med behandlingen rättas (2 kap. 7 och 15 §§). Även dataskyddsförordningen innehåller motsvarande krav på behandling av personuppgifter (artikel 5, se särskilt punkterna a och d). Brottsdatalagens och dataskyddsförordningens krav på behandlingen är alltså väl jämförbara med kraven i personuppgiftslagen och får anses vara tillräckliga för att genomföra rådsbeslutet i denna del utan ytterligare lagstiftningsåtgärder.

Datasäkerhet (artikel 10), loggning (artikel 12) och utbildning av personal (artikel 14)

I artikel 10 i rådsbeslutet finns en tämligen utförlig lista på åtgärder som ska vidtas av medlemsstaterna för att garantera säkerheten för uppgifter i SIS, särskilt vad gäller obehörig åtkomst. Avseende

¹⁸ Prop. 2009/10:86 s. 40.

denna del anförde regeringen att personuppgiftslagens grundläggande krav på åtgärder för att åstadkomma en lämplig säkerhetsnivå och möjligheterna att komplettera med föreskrifter var tillräckliga för att uppfylla kraven i rådsbeslutet. Artikel 10 innehåller också bestämmelser om skyldighet att kunna kontrollera användningen av uppgifter i SIS. Artikel 12 innehåller vidare specifika skyldigheter att logga användningen. Artikel 14 avser ett krav på att personal vid myndigheter som har tillgång till SIS ska ha lämplig utbildning. När det gällde artikel 12 anförde regeringen att loggning av användandet av personuppgifter kan sägas utgöra ett led i att uppfylla de grundläggande kraven i personuppgiftslagen, särskilt 9 och 31 §§. På samma sätt ansågs kravet på utbildad personal vara något som följer av 9 § personuppgiftslagen. Några lagstiftningsåtgärder ansågs därmed inte behövas. En bestämmelse om loggning infördes i förordningen (23 §).¹⁹

Brottsdatalagen föreslås innehålla än mer specifika bestämmelser om datasäkerhet m.m. än personuppgiftslagen. 3 kap. 2 § avser tekniska och organisatoriska åtgärder för att skydda personuppgifter, särskilt mot obehörig eller otillåten behandling. Vidare gäller principerna om inbyggt dataskydd och dataskydd som standard enligt 3 kap. 3 och 4 §§. I den föreslagna brottsdataförordningen, 3 kap. 2 §, finns en bestämmelse om skyldighet att anta och dokumentera interna strategier. I motiveringen till förslaget anges att sådana interna strategier kan avse interna regelverk som behandlar utbildning av personal.²⁰ Att personalen har lämplig utbildning för att kunna följa regelverken som gäller för personuppgiftsbehandling får därmed anses innefattas i kraven på organisatoriska åtgärder för att garantera en författningsenlig behandling.

Även dataskyddsförordningen (se särskilt artikel 24, 25 och 32) innehåller bestämmelser om skyldigheter för den personuppgiftsansvarige som väl motsvarar kraven i personuppgiftslagen och som också i huvudsak motsvarar vad som gäller på direktivets område (principerna om inbyggt dataskydd och dataskydd som standard, artikel 25, gäller exempelvis även enligt förordningen, liksom kravet på organisatoriska åtgärder, artikel 24). Brottsdatalagens och

¹⁹ A. prop. s. 25 f.

²⁰ SOU 2017:29 s. 302.

dataskyddsförordningens reglering i dessa avseenden måste anses ställa sådana krav att rådsbeslutet är genomfört även när dessa regelverk ersätter personuppgiftslagen.

Dataskydd i enlighet med dataskyddskonventionen (artikel 57)

I artikel 57 anges att personuppgifter som behandlas med tillämpning av rådsbeslutet ska skyddas i enlighet med Europarådets konvention av den 28 januari 1981 om skydd för enskilda vid automatisk databehandling av personuppgifter, och senare ändringar av konventionen (dataskyddskonventionen).

Regeringen ansåg att Sverige, genom personuppgiftslagen, kunde anses uppfylla det generella krav på kompletterande lagstiftning som rådsbeslutet ställer i denna artikel.²¹

Ett av de övergripande syftena med både det nya dataskyddsdirektivet och dataskyddsförordningen är att förstärka och harmonisera skyddet för enskilda vid behandling av personuppgifter inom unionen (se särskilt de inledande skälen i båda rättsakterna). Vi menar att man, utan någon mer djupgående analys av dataskyddskonventionen, kan utgå ifrån att de nya EUrättsakterna uppfyller kraven i konventionen (jfr att kravet på adekvat skyddsnivå i tredje länder bl.a. kan bedömas utifrån om landet tillträtt dataskyddskonventionen, direktivets skäl 68 och förordningens skäl 105).

Rätt till information (artikel 58.1)

Vid genomförandet av Schengenkonventionen och senare rådsbeslutet gjordes bedömningen att respektive bestämmelse om rätt till information för den enskilde, som är likalydande i de båda rättsakterna, inte krävde lagstiftningsåtgärder eftersom personuppgiftslagens reglering om rätt till information blev tillämplig även på behandlingen i SIS.²² Rådsbeslutet hänvisar till varje medlemsstats nationella rätt när det gäller informationsskyldighet. Det finns alltså inget hinder emot att det i stället blir brotts-

²¹ Prop. 2009/10:86 s. 45.

²² Prop. 2009/10:86 s. 46.

datalagens, respektive dataskyddsförordningens, bestämmelser om information som i stället ska tillämpas i detta avseende.

I SIS-förordningen finns en bestämmelse med de särskilda tidsfrister för information som följer av rådsbeslutet. Hänvisningen i personuppgiftslagen måste ändras då denna upphör att gälla, vilket behandlas vidare i nästa avsnitt.

Något om tillsyn och sanktioner

Rådsbeslutets artiklar om tillsyn och om sanktioner (artiklarna 60 och 65) genomförs inte i lagen eller förordningen om SIS, utan ansågs uppfyllda genom annan reglering.²³ Som vi anfört i våra allmänna utgångspunkter innebär brottsdatalagen respektive dataskyddsförordningen och dataskyddslagen att ny reglering avseende tillsyn ersätter personuppgiftslagens bestämmelser. Kraven på tillsyn i rådsbeslutet kommer alltså att vara uppfyllda även då personuppgiftslagen upphävs.

De sanktioner som togs upp i samband med genomförandet av rådsbeslutet var exempelvis ansvar för dataintrång och tjänstefel, alltså sanktioner som inte följer av personuppgiftslagens reglering.²⁴ Rådsbeslutets bestämmelse om sanktioner får därför anses genomfört oberoende av att nya generella dataskyddsregler införs i stället för personuppgiftslagen.

7.4 Överväganden om och förslag till författningsändringar

Förslag: I lagen om SIS införs en bestämmelse som anger att lagen gäller utöver brottsdatalagen. Av bestämmelsen ska framgå att regleringen i lagen om SIS som gäller användningsbegränsningar och känsliga personuppgifter tillämpas i stället för bestämmelser i brottsdatalagen om känsliga personuppgifter, vidarebehandling och överföring till tredje land. I lagen om SIS införs vidare en bestäm-

²³ A. prop. s. 53. Frågan om tillsyn berördes inte i denna proposition, utan bedömningen av behovet av lagstiftningsåtgärder får anses framgå av den tidigare propositionen om genomförandet av Schengenkonventionen, prop. 1999/2000:64 s. 155.

²⁴ Prop. 2009/10:86 s. 53.

melse som upplyser om att lagen kompletterar dataskyddsförordningen avseende sådan personuppgiftsbehandling som inte omfattas av brottsdatalagens tillämpningsområde och att dataskyddslagen också gäller för sådan behandling. I bestämmelsen anges att bestämmelser om känsliga personuppgifter i lagen om SIS tillämpas i stället för 3 kap. 4 § dataskyddslagen om myndigheters möjligheter att behandla sådana uppgifter.

Bestämmelserna om rättelse och radering (15 §) samt bestämmelsen om överklagande av beslut om sådana åtgärder (17 §) upphävs.

Bestämmelsen om skadestånd i lagen om SIS (16 §) ändras så att en hänvisning görs till brottsdatalagen i stället för personuppgiftslagen såvitt avser personuppgiftsbehandling i SIS som omfattas av brottsdatalagens tillämpningsområde.

I förordningen tas hänvisningen till personuppgiftslagen bort i bestämmelsen om information på begäran av den enskilde (21 §). I 22 § i förordningen utgår hänvisningen till 15 § i lagen.

Skälen för förslaget:

Upplysande bestämmelser om kompletterande reglering

Som vi redan redogjort för menar vi att lagen och förordningen om SIS kommer att komplettera både brottsdatalagen och dataskyddsförordningen, beroende på vilket syfte behandlingen i SIS har. Lagen om SIS innehåller i dag ingen bestämmelse som upplyser om förhållandet till personuppgiftslagen.²⁵ Vi anser att det nu finns anledning att införa bestämmelser som upplyser om vilken reglering som gäller på en generell nivå. Det är särskilt motiverat med sådana bestämmelser eftersom både brottsdatalagen och dataskyddsförordningen kommer att bli tillämpliga på personuppgiftsbehandlingen i SIS (jfr vad vi anför om belastningsregistret, avsnitt 5.5).

Även dataskyddslagen bör gälla för personuppgiftsbehandlingen i SIS som omfattas av dataskyddsförordningen, se vidare våra allmänna överväganden, avsnitt 2.5.9.

²⁵ Jfr prop. 2009/10:86 s. 46.

Avvikelser i förhållande till brottsdatalagen

Som vi redan redogjort för är regleringen i SIS som avser känsliga personuppgifter och användningsbegränsningar förenliga med det nya dataskyddsdirektivet. I förhållande till brottsdatalagen innebär dock lagen om SIS vissa avvikelser. Visserligen följer det av brottsdatalagens subsidiaritet att avvikande bestämmelser i annan lag ska tillämpas i stället för brottsdatalagen (1 kap. 5 §). Vi menar att det blir tydligare för tillämparen att uttryckligen ange vilka bestämmelser i lagen om SIS som ska gälla i stället för vissa bestämmelser i brottsdatalagen.

Lagen om SIS reglerar uttömmande användningen av känsliga personuppgifter i registret. Brottsdatalagens bestämmelser i 2 kap. 11 § innebär däremot en generell möjlighet att behandla sådana personuppgifter under vissa förutsättningar. Den ska därmed inte tillämpas. När det gäller de användningsbegränsningar som finns i 10 och 13 §§ lagen om SIS innebär dessa, som redogjorts för i föregående avsnitt, en inskränkning i de möjligheter till behandling som följer av det nya dataskyddsdirektivet och därmed av brottsdatalagen. Alltså måste dessa bestämmelser tillämpas i stället för de generella bestämmelserna om vidarebehandling i 2 kap. 4 och 22 §§ brottsdatalagen. Förbudet mot överföring till tredje land och internationella organisationer som följer av 10 § lagen om SIS ska också tillämpas i stället för 8 kap. i brottsdatalagen, som under vissa förutsättningar medger sådana överföringar.

När det gäller gallring innebär regleringen i lagen om SIS en viss dubbelreglering i förhållande till brottsdatalagen. Bestämmelsen om bevarande (11 § i lagen) ger till viss del uttryck för samma sak som 2 kap. 17 § brottsdatalagen. Det finns dock ingen motsättning mellan bestämmelserna och det torde inte innebära några tillämpningsproblem att de tillämpas parallellt.

Avvikelser i förhållande till dataskyddslagen

I 3 kap. 3 § dataskyddslagen finns bestämmelser som ger myndigheter en generell möjlighet att behandla känsliga personuppgifter under vissa förutsättningar. Lagen om SIS innehåller som redan redogjorts för, en särreglering av möjligheterna att behandla sådana uppgifter. Att lagen om SIS i det avseendet ska tillämpas i stället för dataskyddslagen bör framgå uttryckligen av den bestämmelse

som i övrigt upplyser och att dataskyddsförordningen och dataskyddslagen gäller. Även dataskyddslagen är subsidiär till annan författning, men vi menar att lagen om SIS blir tydligare om avvikelserna uttryckligen pekats ut i författningen.

Skadestånd

I lagen om SIS finns, liksom i de flesta andra registerförfattningar, en bestämmelse som hänvisar till 48 § personuppgiftslagen (16 §). För att även behandling enligt lagen eller förordningen om SIS som sker inom brottsdatalagens tillämpningsområde ska täckas av skadeståndsansvar måste bestämmelsen i 16 § hänvisa till 7 kap. 1 § brottsdatalagen i stället för 48 § personuppgiftslagen (se även våra allmänna överväganden, avsnitt 2.6.7). Det kan anmärkas att rådsbeslutet när det gäller skadestånd inte ställer några mer specifika krav utan hänvisar till aktuell nationell rätt (artikel 64).

Som vi tidigare angett menar vi att det inte behövs några hänvisningar till dataskyddsförordningens skadeståndsreglering i registerförfattningar (avsnitt 2.5.9).

Rättelse och radering samt överklagande av sådana beslut

Som vi redan anfört menar vi att den nuvarande regleringen av rättelse och radering i 15 § lagen om SIS inte utgör någon skillnad i sak mot de bestämmelser som genomför det nya dataskyddsdirektivet i dessa delar, dvs. 4 kap. 9 och 10 §§ brottsdatalagen, och inte heller i förhållande till dataskyddsförordningens bestämmelser om rättelse och radering. För behandling inom det nya dataskyddsdirektivets tillämpningsområde hade bestämmelsen i lagen om SIS i och för sig kunnat behållas med tillämpning av artikel 60 i det nya dataskyddsdirektivet. Det finns samtidigt inget hinder emot att låta brottsdatalagens reglering bli gällande i stället. Inom dataskyddsförordningens tillämpningsområde måste däremot förordningen tillämpas direkt. Vi menar att det lämpligaste sättet att anpassa regleringen i lagen om SIS och samtidigt genomföra rådsbeslutet på ett korrekt sätt är att upphäva 15 §. Brottsdatalagen, dataskyddsförordningen och dataskyddslagen tillämpas då med avseende på rättelse, radering och överklagande av sådana beslut. Om 15 § upphävs fyller inte längre 17 § någon funktion och bör även den upphävas.

Ändringar i förordningen om SIS

Enligt artikel 58.1 i rådsbeslutet ska nationell rätt tillämpas avseende personers åtkomst till uppgifter om sig själva. Själva rätten till information är alltså genomförd genom att 25–27 §§ personuppgiftslagen tillämpas på personuppgiftsbehandling i SIS. I förordningens 21 § genomfördes rådsbeslutets bestämmelse om tidsfrister för sådant informationslämnande. För information om vidtagna åtgärder avseende rättelse m.m. gäller också vissa absoluta tidsfrister enligt rådsbeslutet. Rådsbeslutet i dessa delar genomfördes i 22 § i förordningen.²⁶

När personuppgiftslagen nu ska upphävas blir brottsdatalagen respektive dataskyddsförordningen tillämplig på information om behandling. Det finns inga särskilda tidsfrister i brottsdatalagen eller dataskyddsförordningen. Att behålla de tidsfrister som finns i 21 § förordningen om SIS får anses vara en tillåten precisering i förhållande till både det nya dataskyddsdirektivet och dataskyddsförordningen. Hänvisningen till personuppgiftslagen måste dock utgå. Vi bedömer att den inte behöver ersättas med nya hänvisningar till brottsdatalagen respektive dataskyddsförordningen.

Tidsfristen i 22 § i förordningen gäller information om vidtagna åtgärder enligt 15 § lagen om SIS. Vi bedömer att bestämmelsen i sak kan behållas, eftersom den inte strider mot någon reglering i vare sig det nya dataskyddsdirektivet eller dataskyddsförordningen, utan preciserar den enskildes rättigheter i enlighet med en EUrättsakt. Däremot kan hänvisningen till 15 § i bestämmelsen inte behållas då denna paragraf upphävs. Vi bedömer att inte heller denna hänvisning behöver ersättas med hänvisningar till brottsdatalagen eller dataskyddsförordningen.

Bestämmelserna i 21 och 22 § i förordningen blir alltså tillämpliga oavsett vilken övergripande reglering (brottsdatalagen eller dataskyddsförordningen) som ska anses tillämplig på den enskildes begäran om information, rättelse eller annan åtgärd.

²⁶ Prop. 2009/10:86 s. 46 f.

8 Förordningen om förenklat uppgiftsutbyte mellan brottsbekämpande myndigheter i Europeiska unionen

8.1 Om författningen

Bakgrund

Förordningen (2008:1396) om förenklat uppgiftsutbyte mellan brottsbekämpande myndigheter i Europeiska unionen (kallas *förordningen om uppgiftsutbyte* eller *förordningen* i det följande) genomför en EU-rättsakt; ett av rådets rambeslut som avser informationsutbyte i brottsbekämpande syfte. Följande beskrivning av bakgrunden och innehållet i rambeslutet samt det svenska genomförandet ges i regeringens proposition 2009/10:85 Integritet och effektivitet i polisens brottsbekämpande verksamhet.

Den tillgänglighetsprincip som är väsentlig i EU:s arbete för att utveckla informationsutbytet är en av hörnstenarna i rambeslutet om förenklat informations- och underrättelseutbyte. Rådets rambeslut 2006/960/RIF av den 18 december 2006 om förenklat informations- och underrättelseutbyte mellan de brottsbekämpande myndigheterna i Europeiska unionens medlemsstater kom till efter ett svenskt initiativ. Rambeslutet innebär att brottsbekämpande myndigheter i medlemsstaterna redan på underrättelsestadiet, och över myndighetsgränserna, snabbt ska kunna utbyta befintlig information och befintliga underrättelser. Genom rambeslutet åtar sig medlemsstaterna bl.a. dels att på begäran av en annan stat lämna viss information, dels att spontant lämna vissa uppgifter.

Rambeslutet har genomförts i svensk rätt genom förordningen (2008:1396) om förenklat uppgiftsutbyte mellan brottsbekämpande myndigheter i Europeiska unionen, som trädde i kraft den 1 februari 2009. Förordningen, som bygger på förutsättningen att gällande svensk rätt redan medger utlämnande av sådana uppgifter som ska utbytas enligt rambeslutet, innehåller framför allt bestämmelser om förfarandet i samband med uppgiftsutbytet.

En närmare beskrivning av rambeslutet och överväganden om genomförandet i svensk rätt finns i promemorian *Enklare informationsutbyte i brottsbekämpningen inom EU* (Ds 2008:72).

Kort om innehållet i förordningen om uppgiftsutbyte

Förordningen innehåller 12 paragrafer. Som beskrivs i citatet ovan avser de flesta bestämmelser om förfarandet i samband med uppgiftsutbytet. Svenska myndigheter är enligt förordningen skyldiga att lämna uppgifter under vissa förutsättningar, både efter begäran och spontant, om det finns sakliga skäl att anta att ett uppgifts-utlämnande kan bidra till att bekämpa brott (3–5 §§). Bestämmelserna i 6 § tar upp möjligheten att ställa upp villkor vid ett svenskt uppgiftsutlämnande. Förordningen om uppgiftsutbyte innehåller vidare bestämmelser om tidsfrister för informationslämnande (7–9 §§). Bestämmelserna i 10–12 §§ rör svenska myndigheters begäran om information och en hänvisning till att det i annan lagstiftning finns bestämmelser som begränsar möjligheten att utnyttja uppgifter som överförts till svenska myndigheter.

Inledningsvis i förordningen finns bestämmelser som hänvisar till de EU-rättsakter som genomförs genom förordningen (1 §). I 1 a § finns en erinran om att det i lagen (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen, och i föreskrifter som regeringen har meddelat i anslutning till den lagen, finns särskilda bestämmelser om behandling av personuppgifter som inom ramen för polissamarbete eller straffrättsligt samarbete har gjorts tillgängliga av vissa uppräknade stater.

Förslag till ändringar i SOU 2017:29

Utredningen om 2016 års dataskyddsdirektiv har lagt fram författningsförslag avseende förordningen om förenklat uppgiftsutbyte i sitt delbetänkande *Brottsdatalag* (2017:29). Deras författningsförslag gäller ett tillägg till 6 § som erinrar om brottsdatalagens reglering av användningsbegränsningar i vissa fall.¹

8.2 Överväganden och förslag

Förslag och bedömning: Det nya dataskyddsdirektivet föranleder, utöver upphävande av 1 a §, inga ändringar i förordningen om förenklat uppgiftsutbyte.

Skälen för förslaget och bedömningen: Av 3, 4 och 10 §§ i förordningen framgår att uppgiftsutbyte enligt förordningen avser ett utbyte mellan behöriga myndigheter i det nya dataskyddsdirektivets mening och för sådana syften som avgränsar direktivets tillämpningsområde. I den mån ett uppgiftsutbyte innebär personuppgiftsbehandling som i övrigt omfattas av direktivet (helt eller delvis automatiserad etc.) berörs alltså regleringen av det nya dataskyddsdirektivets tillämpningsområde. Det bakomliggande rambeslutet är samtidigt en sådan EU-rättsakt som enligt artikel 60 ska gälla i stället för det nya dataskyddsdirektivet.²

Förordningen om förenklat uppgiftsutbyte avser, som beskrivits ovan, i första hand procedurregler för hur uppgiftsutbytet ska gå till. Som redan redogjorts för bygger förordningen på förutsättningen att uppgiftslämnande enligt rambeslutet i sig är tillåtet enligt annan relevant svensk lagstiftning, exempelvis polisdatalagen (2010:361). Förordningen innehåller inga dataskyddsbestämmelser som avser personuppgifter som lämnats från en annan stat. Bestämmelser om användningsbegränsningar för sådana uppgifter finns i annan lag, vilket erinras om i 11 §. Enligt 6 § i förordningen finns också möjlighet för en svensk myndighet att ställa upp villkor för användandet av uppgifter som lämnas till en annan medlems-

¹ SOU 2017:29 s. 77 och 290.

² Jfr SOU 2017:29 s. 156.

stat. Utredningen om 2016 års dataskyddsdirektiv har gjort bedömningen att möjligheten att ställa upp användningsbegränsningar som följer av tidigare EU-rättsakter inom området för polisiärt samarbete kan behållas i enlighet med artikel 60 i det nya dataskyddsdirektivet.³ Vi gör samma bedömning och hänvisar i övrigt till utredningens förslag i denna del, jfr avsnittet ovan.

Artikel 8 i rambeslutet, som avser dataskydd, anger i princip att befintliga dataskyddsbestämmelser i medlemsstaterna ska tillämpas även på informationsutbyte enligt rambeslutet och att uppgifter som samlas in med stöd av rambeslutet inte ska ha ett sämre skydd än uppgifter som samlas in nationellt. I den tidigare nämnda promemorian gjordes bedömningen att den svenska dataskyddsregleringen uppfyllde åtagandena i rambeslutet.⁴ Det torde vara förenligt med rambeslutets dataskyddsbestämmelser att tillämpa brottsdatalagen på förekommande personuppgiftsbehandling i anledning av informationsutbyte enligt rambeslutet. Det finns heller inte någon motsättning mellan rambeslutet och förordningen om uppgiftsutbyte å ena sidan och det nya dataskyddsdirektivet å den andra. Förordningen om uppgiftsutbyte innehåller i dag ingen upplysande bestämmelse om förhållandet till personuppgiftslagen och inte heller några andra hänvisningar till denna lag. Som påpekats ovan avser författningen i huvudsak inte heller att reglera frågor om dataskydd. Med beaktande av detta menar vi att det inte behövs någon upplysande bestämmelse som anger att förordningen om uppgiftsutbyte gäller utöver brottsdatalagen.

Den ändring som behövs i förordningen avser 1 a §, som hänvisar till lagen (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen. Lagen och föreskrifter med stöd av lagen kommer att upphävas som en konsekvens av att det nya dataskyddsdirektivet genomförs, se vidare avsnitt 2.6.5. Vi föreslår därför att 1 a § ska upphöra att gälla.

³ SOU 2017:29 s. 290 f.

⁴ Ds 2008:72 s. 68.

9 Förordningen om behandling av personuppgifter i Nationellt forensiskt centrums uppdragsverksamhet

9.1 Om författningen

Bakgrund – verksamheten vid Nationellt forensiskt centrum

Nationellt forensiskt centrum är sedan den 1 januari 2015 en del av Polismyndigheten. Då trädde författningsändringar i kraft som innebar en sammanslagning av Rikspolisstyrelsen, polismyndigheterna och Statens kriminaltekniska laboratorium till en myndighet, Polismyndigheten. Vid sammanslagningen bytte alltså Statens kriminaltekniska laboratorium namn till Nationellt forensiskt centrum (kallas *NFC* i det följande).¹

NFC:s verksamhet regleras närmare i förordningen (2014:1102) med instruktion för Polismyndigheten. Enligt 11 § ska NFC utföra forensiska undersökningar som föranleds av misstanke om brott eller brottslig verksamhet och bedriva annan verksamhet som har samband med sådana undersökningar. Nationellt forensiskt centrum ska också enligt 12 § bedriva forensisk forskning och utveckling inom sitt ansvarsområde och samla, bearbeta och offentliggöra resultat inom området.

Tyngdpunkten i Nationellt forensiskt centrums verksamhet är de forensiska undersökningar som utförs åt rättsväsendet. Begäran om forensisk undersökning kommer i första hand från andra enheter inom Polismyndigheten.²

¹ Prop. 2014/15:94 s. 36.

² Prop. 2014/15:94 s. 38.

Enligt 11 § tredje stycket förordningen med instruktion för Polismyndigheten får Nationellt forensiskt centrum – om dess utrustning och förhållandena i övrigt medger det – även utföra andra undersökningar än de som ingår i de primära uppgifterna (uppdragsverksamhet). Verksamheten, som är avgiftsfinansierad, utgör en mycket liten del av centrumets verksamhet. Uppdragsgivare är bl.a. försäkringsbolag och privatpersoner. Offentliga försvarare vänder sig ibland för sina klienters räkning till centrumet med uppdrag. Det förekommer också att myndigheter som inte bedriver brottsbekämpande verksamhet vänder sig till centrumet för olika typer av undersökningar, t.ex. Statens haverikommission, Migrationsverket och Försvarsmakten. Centrumet utför regelbundet handstilsundersökningar åt det isländska rättsväsendet.³

Regleringen av personuppgiftsbehandlingen vid NFC

Den personuppgiftsbehandling som är nödvändig för utförandet av NFC:s huvudsakliga verksamhet, alltså uppdrag som kommer från rättsväsendet, regleras i 5 kap. polisdatalagen (2010:361).

Personuppgiftsbehandlingen för uppdragsverksamheten regleras i stället i förordningen (2015:476) om personuppgiftsbehandling i Nationellt forensiskt centrums uppdragsverksamhet (kallas *förordningen om uppdragsverksamheten vid NFC* eller *förordningen* i det följande). Regeringen konstaterade i sina överväganden avseende 5 kap. polisdatalagen att denna reglering inte skulle bli tillämplig på uppdragsavtalen, eftersom uppdragsgivaren anlitar NFC på civilrättslig grund. När det gällde möjligheten för NFC att behandla personuppgifter med anledning av uppdragsavtalen ansåg regeringen dock att det inte var tillräckligt att hänvisa till 10 § a personuppgiftslagen (behandling som är nödvändig för att fullgöra ett avtal med den registrerade) eftersom den som begär undersökningen och är avtalspart inte alltid är den som personuppgiftsbehandlingen rör. Regeringens bedömning var att det krävdes en

³ A. prop. s. 41. Av propositionen framgår att vissa uppdrag från brottsbekämpande myndigheter tidigare ansågs ingå i uppdragsverksamheten på grund av att de var avgiftsfinansierade, exempelvis uppdrag från Skatteverket eller Kustbevakningen. Sådana uppdrag hänfördes dock till samma reglering som för Polismyndighetens uppdrag i brottsbekämpande syften, vilket framgår av 5 kap. 1 § 2 polisdatalagen, jfr a. prop. s. 60 f.

särskild reglering för att ge NFC möjlighet att behandla personuppgifter i uppdragsverksamheten även med avseende på andra personer än uppdragsgivaren. Eftersom uppdragsverksamheten är mycket begränsad, rör få personer och i liten utsträckning sköts automatiserat, ansåg regeringen att behandlingen inte behövde regleras i lag utan kunde meddelas på lägre föreskriftsnivå.⁴

Innehållet i förordningen om uppdragsverksamheten vid NFC

Förordningen innehåller sex paragrafer. I den första anges tillämpningsområdet för förordningen – den tillämpas på helt eller delvis automatiserad behandling av personuppgifter vid undersökningar som NFC utför på uppdrag av andra än de myndigheter eller organ som anges i 5 kap. 1 § polisdatalagen. I 3 § regleras personuppgiftsansvaret för behandlingen och i 4 § tillåtna ändamål för den. Tillgången till personuppgifter, 5 §, regleras på samma sätt som i flertalet andra registerförfattningar för myndigheter med brottsbekämpande uppdrag – den ska vara begränsad till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter.

I övrigt är personuppgiftslagen tillämplig på personuppgiftsbehandlingen i uppdragsverksamheten, vilket också följer av 2 §. I 6 § anges att personuppgiftslagens bestämmelser om rättelse och skadestånd ska tillämpas även på personuppgiftsbehandling enligt förordningen.

9.2 Överväganden och förslag

Bedömning: Personuppgiftsbehandlingen i enlighet med förordningen om uppdragsverksamheten vid NFC omfattas av dataskyddsförordningens tillämpningsområde. Regleringen uppfyller kraven på rättslig grund i dataskyddsförordningens artikel 6.1 och 6.3. Bestämmelserna i 1 § och 3–5 §§ i förordningen är förenliga med dataskyddsförordningen i enlighet med artikel 6.2 och behöver inte ändras som en följd av att dataskyddsförordningen ska börja tillämpas.

⁴ Prop. 2014/15:94 s. 79 f.

Ingen ny reglering av rättelse eller skadestånd behövs i förordningen. Det behövs inte heller någon reglering som inskränker tillämpningen av dataskyddsförordningens artiklar 16–21.

Förslag: I stället för det nuvarande innehållet i 2 §, som reglerar förhållandet till personuppgiftslagen, införs en upplysande bestämmelse om att förordningen om uppdragsverksamheten vid NFC kompletterar dataskyddsförordningen och att dataskyddslagen gäller. Rubriken till 2 § ändras i enlighet med detta. Förordningens 6 § och rubriken före paragrafen upphävs. Hänvisningen till polisdatalagen i 1 § ändras i enlighet med förslaget till polisens brottsdatalag.

Skälen för bedömningen och förslaget:

Dataskyddsförordningen är den tillämpliga EU-rättsakten

Sedan omorganisationen av polisen är NFC en del av Polismyndigheten. Personuppgiftsbehandlingen som sker i brottsbekämpande syfte, dvs. utförs inom ramen för uppdrag från andra brottsbekämpande myndigheter i enlighet med 5 kap. 1 § polisdatalagen, omfattas av det nya dataskyddsdirektivets och brottsdatalagens tillämpningsområde. Uppdragsverksamheten omfattas däremot inte av NFC:s uppdrag som en brottsbekämpande myndighet och sker inte heller i syfte att bekämpa brott. Det är därmed dataskyddsförordningen som ska tillämpas på personuppgiftsbehandlingen i uppdragsverksamheten. Detta gäller även om uppdraget avser en undersökning som kan komma att få betydelse för en brottmålsprocess, exempelvis för att en misstänkt gett uppdraget.⁵

Rättslig grund för personuppgiftsbehandlingen

Personuppgiftsbehandling som är nödvändig för att fullgöra ett avtal med den registrerade som part är laglig enligt artikel 6.1 b dataskyddsförordningen, på samma sätt som enligt det gamla

⁵ SOU 2017:29 s. 190.

dataskyddsdirektivet och personuppgiftslagen. Denna grund kan dock, som regeringen påpekade enligt redogörelsen ovan, inte åberopas för att behandla uppgifter om andra personer än uppdragsgivaren. I vissa fall skulle personuppgiftsbehandling avseende andra personer än uppdragsgivaren kunna motiveras med att behandlingen behövs för att skydda en enskild persons grundläggande intressen (artikel 6.1 d). Det är samtidigt tveksamt vilka intressen som skulle kunna fall in under begreppet *grundläggande intressen*.

Myndigheters uppdragsverksamhet kan också, som Dataskyddsutredningen anför, i vissa fall anses vara en uppgift av allmänt intresse, alltså laglig enligt 6.1 e.⁶ Att andra än rättskedjans myndigheter, både andra myndigheter, företag och enskilda, har möjlighet att ta del av den särskilda kompetens som NFC har, anser vi vara ett allmänt intresse. Att regeringen funnit för gott att införa en författningsreglering för att möjliggöra en personuppgiftsbehandling, talar också för detta. Det är alltså artikel 6.1 e som får anses tillämplig på personuppgiftsbehandlingen i uppdragsverksamheten. Eftersom NFC:s uppdragsverksamhet är författningsreglerad i Polismyndighetens instruktion (se ovan) och personuppgiftsbehandlingen i sig också är reglerad i förordningen om uppdragsverksamheten vid NFC, är den rättsliga grunden fastställd i nationell rätt på sätt som krävs enligt artikel 6.3.

Regleringen är i huvudsak förenlig med dataskyddsförordningen

Bestämmelserna 1 § och 3–5 §§ är förenliga med dataskyddsförordningen i enlighet med artikel 6.2, eftersom de preciserar behandlingen av personuppgifter på ett tillåtet sätt (se vidare avsnitt 2.5.4). Det kan anmärkas att 4 § tredje stycket utesluter annan behandling än för de föreskrivna ändamålen. De är alltså inte möjligt för NFC att självständigt tillämpa finalitetsprincipen och utvidga behandlingen till andra ändamål än de ursprungliga ändamålen, även om sådana skulle vara förenliga med dessa. En sådan inskränkning får, som utvecklats i avsnitt 2.5.3, anses förenlig med dataskyddsförordningen när det gäller myndigheters verksamhet.

⁶ SOU 2017:39 s. 125.

Förhållandet till dataskyddsförordningen och dataskyddslagen samt hänvisningen till polisens brottsdatalog

I 2 § finns en hänvisning till personuppgiftslagen och bestämmelsen måste alltså ändras. Eftersom förordningen för närvarande innehåller denna bestämmelse som klargör förhållandet till personuppgiftslagen, anser vi att det är lämpligt att i stället införa bestämmelser som visar på förhållandet till dataskyddsförordningen och dataskyddslagen. Om utformningen av bestämmelser som upplyser om dataskyddslagen, se våra allmänna överväganden, avsnitt 2.5.9.

I 1 §, som avgränsar förordningens tillämpningsområde, finns en hänvisning till polisdatalagen. Utredningen om 2016 års dataskyddsdirektiv föreslår ändringar i polisdatalagen, bl.a. kommer författningen att få ett nytt namn. Utredningen har redan föreslagit en ändring i enlighet med detta i förordningen om NFC:s uppdragsverksamhet.⁷ För helhetens skull tar vi upp samma ändring i våra författningsförslag.

Bestämmelsen om rättelse och skadestånd upphävs

När det gäller rättelse och skadestånd finns i dag en hänvisning till personuppgiftslagens bestämmelser i förordningens 6 §. I stället för personuppgiftslagen kommer dataskyddsförordningen att bli direkt tillämplig. Som vi anför i våra allmänna överväganden (avsnitt 2.5.9) finns det inget behov av att hänvisa till dataskyddsförordningen för att bestämmelserna i den om rättelse och skadestånd ska bli tillämpliga. Av dataskyddslagens 8 kap. 1 § kommer dessutom att framgå att skadestandsregleringen gäller också för behandling som utförs med stöd av en registerförfattning.

⁷ SOU 2017:74 s. 270.

Behov av inskränkningar i de rättigheter som följer av artikel 16–21?

Enligt vår redogörelse i avsnitt 2.5.8 ser vi inga generella skäl att inskränka den enskildes rättigheter som följer av dataskyddsförordningens artikel 16–21. Det har inte heller framkommit några skäl som särskilt hänför sig till NFC:s uppdragsverksamhet som föranleder någon annan bedömning. Det är tänkbart att det finns uppdrag där en enskild motsätter sig personuppgiftsbehandling, exempelvis eftersom det inte ligger i den enskildes intresse att den undersökning uppdraget avser blir utförd. Detta skulle då vara andra enskilda än uppdragsgivaren, om det är en privatperson – uppdragsgivaren kan ju alltid avbryta personuppgiftsbehandlingen genom att dra tillbaka uppdraget. Som redan beskrivits finns det en stor variation i NFC:s uppdragsverksamhet. Detta gör det särskilt svårt att förutse i vilka situationer det skulle vara motiverat att göra inskränkningar i den enskildes rättigheter. Sådana inskränkningar måste, som tidigare påpekats, kunna motiveras utifrån ett eller flera särskilda syften som anges i artikel 23.1. Med beaktande av detta, och det vi anført i våra allmänna överväganden, föreslår vi inga sådana inskränkningar.

10 Lagen om hotell- och pensionatrörelse

10.1 Om författningen

Bakgrund

Lagen (1966:742) om hotell- och pensionatrörelse hade från början förordningsform och innehöll något fler bestämmelser än dagens lag. Det huvudsakliga innehållet i och syftet med lagen är dock detsamma som i den ursprungliga förordningen. Genom förordningen infördes en tillståndsplikt för att driva hotell- och pensionatrörelse. Vidare infördes grundläggande krav på rörelsen och på den som driver rörelsen. Departementschefen anförde följande.

God ordning i hotell har som framhållits i departementspromemorian betydelse för bl.a. hotellgästernas trygghet till liv och hälsa. Åtskilliga ordningsföreskrifter som behövs för hotell har i själva verket till syfte att främja brandskydd och hälsovård. I dessa hänseenden bör ordningsintressena enligt min mening tillgodoses enligt brand- och hälsovårdslagstiftningen, på de sätt som jag redogjort för i det föregående. Fullständig garanti för att bestämmelserna i denna lagstiftning efterlevs i den mån det ankommer på hotellinnehavaren eller hotellföreståndare kan självfallet inte vinnas. Väsentlig säkerhet härvidlag kan dock uppnås med en ordning som innebär att hotellverksamhet får utövas endast av ansvarskännande och ordentliga personer.

God ordning fordras även i det hänseendet att hotell inte får bli tillhåll för kriminellt belastade eller andra asociala individer. Det är ett samhällsintresse att hotell inte drivs på ett sätt som underlättar för sådana element att leva i anonymitet. God ordning i hotell måste upprätthållas också som ett medel att förhindra prostitution. Det bör således av den som driver eller förestår hotell fordras att han utövar viss kontroll över gästerna.

Även av nu anförda skäl måste enligt min mening fordras ansvarskänsla och ordentlighet av den som driver eller förestår hotellrörelse.¹

Det kan anmärkas att lagen om hotell- och pensionatrörelse från början innehöll flera bestämmelser om skyldighet att föra en gästförteckning. Med tiden ansågs den lagstadgade skyldigheten ha blivit överflödig, eftersom hotellen ändå torde ha uppgifter om sina gäster för rörelsens skull. Rikspolisstyrelsen menade också att gästförteckningarnas värde från spaningssynpunkt därtill var begränsat eftersom hotellgäster ändå inte hade skyldighet att legitimera sig.²

Innehållet i lagen

I lagens 1 § avgränsas tillämpningsområdet. Bestämmelserna i 2–4 §§ avser tillståndsplikten och krav på att rörelse som drivs i bolagsform ska ha en föreståndare. Förutsättningarna för tillstånd framgår av 2 § och avser bl.a. att det inte ska finnas anledning att anta att rörelsen kommer att drivas så att fara för allmän ordning och säkerhet uppkommer. I 5 § finns bestämmelser om ansökan om tillstånd och bevis om tillstånd, om sådant beviljas. Bestämmelserna i 6–8 §§ reglerar vad som gäller då förutsättningarna för de meddelade tillståndet förändras, exempelvis om föreståndare avlider eller får förvaltare eller att bolaget som driver rörelsen sätts i konkurs.

Av 9 § följer att Polismyndigheten ska föra ett register över beviljade tillstånd.

Under rubriken *Ordning och säkerhet* finns numera endast två gällande paragrafer, 10 och 12 §§. Övriga (11 § och 13–15 §§) är upphävda, jfr under rubriken ovan. De kvarvarande kraven på rörelsen gäller dels att den inte får drivas så att fara för allmän ordning och säkerhet uppkommer, dels att utrymningsvägar ska vara tydligt markerade.

¹ Prop. 1966:124 s. 37.

² Prop. 1979/80:123 s. 5 f. Bestämmelser om skyldighet att föra gästförteckning fanns i 13–15 §§ och 17 §, paragraferna upphävdes i enlighet med förslaget i propositionen (SFS 1980:345). Genom en senare lagändring upphävdes ytterligare en paragraf, 11 §, som avsåg elsäkerhet, SFS 2016:741, prop. 2015/16:163.

Slutligen innehåller lagen ansvarsbestämmelser och bestämmelser om tillsyn, förutsättningar för att dra tillbaka tillstånd samt en bestämmelse om överklagande av Polismyndighetens beslut som fattas enligt lagen (16–22 §§).

10.2 Överväganden

Bedömning: Personuppgiftsbehandlingen i registret över hotell- och pensionatrörelse och annan förekommande personuppgiftsbehandling i anledning av ansökan om tillstånd omfattas av dataskyddsförordningens tillämpningsområde. Personuppgiftsbehandlingen i enlighet med lagen om hotell- och pensionatrörelse uppfyller kraven på rättslig grund i dataskyddsförordningens artikel 6.1 och 6.3. Regleringen behöver inte ändras som en följd av att dataskyddsförordningen ska börja tillämpas.

Skälen för bedömningen:

Dataskyddsförordningen är den tillämpliga EU-rättsakten

Som redan redogjorts för gäller regleringen i lagen om hotell- och pensionatrörelse i huvudsak inte dataskydd. Lagens huvudsakliga innehåll är istället de materiella reglerna för den tillståndsplikt som ansetts nödvändig att införa samt regler för tillsyn m.m. Den bestämmelse som får anses avse personuppgiftsbehandling är 9 §, som anger att ett register ska föras. Det finns inga närmare bestämmelser om att registret ska innehålla personuppgifter, men eftersom en hotell- och pensionatrörelse kan drivas av enskilda näringsidkare eller annars ska ha en föreståndare torde uppgifterna i registret alltid innehålla personuppgifter. Lagen förutsätter inte att registret förs automatiserat. Även manuella register omfattas dock av både det nya dataskyddsdirektivets och dataskyddsförordningens tillämpningsområde. Den praktiska hanteringen av tillstånd m.m. hos Polismyndigheten innebär därtill en automatiserad behandling.

Som redogjorts för är det grundläggande syftet bakom tillståndsplikten att fara för allmän ordning och säkerhet inte ska uppstå. Det nya dataskyddsdirektivet omfattar personuppgifts-

behandling som är nödvändig i syfte att bl.a. förebygga hot mot allmän ordning och säkerhet.

När det gäller allmän ordning och säkerhet har Utredningen om 2016 års dataskyddsdirektiv tolkat direktivet så att det är *upprätthållande* av allmän ordning och säkerhet som omfattas av tillämpningsområdet. I att upprätthålla allmän ordning och säkerhet ligger att vidta faktiska åtgärder vid konkreta ordningsstörningar eller konkreta risker för att sådana störningar ska uppstå. Kontrollverksamhet eller allmän övervakning omfattas inte av det nya dataskyddsdirektivets tillämpningsområde enligt utredningens mening.³

Med ledning av denna bedömning anser vi att tillståndsplikten och registreringen av hotell- och pensionatrörelser inte kan anses utgöra ett upprätthållande av allmän ordning och säkerhet, utan snarast är att likställas med en kontroll- och övervakningsverksamhet. Personuppgiftsbehandlingen i det författningsreglerade registret och annan personuppgiftsbehandling i anledning av tillståndskravet är därmed sådan behandling som omfattas av dataskyddsförordningens tillämpningsområde.

Dataskyddsförordningens krav på rättslig grund

Tillståndsplikten för hotell- och pensionatrörelse har införts för att motverka störningar av allmän ordning och säkerhet, alltså med ett allmänintresse som grund. Att pröva ansökningar om tillstånd, meddela beslut m.m. som krävs för att upprätthålla tillståndsplikten får alltså anses vara en uppgift av allmänt intresse. Den personuppgiftsbehandling som behövs för att utföra uppgiften, exempelvis automatiserad behandling av ansökningar om tillstånd, har därmed en rättslig grund i enlighet med artikel 6.1 e. Att föra ett register är också en behandling som behövs för att upprätthålla tillståndsplikten och därmed ingår en sådan behandling i uppdraget av allmänt intresse. Förandet av registret är också en skyldighet för polisen och därmed en rättslig förpliktelse, en annan grund för laglig behandling, enligt artikel 6.1 c.

³ SOU 2017:29 s. 167, 184 och 227 f.

Eftersom uppgiften av allmänt intresse och den rättsliga förpliktelsen är författningsreglerad är den rättsliga grunden också fastställd i nationell rätt på sätt som krävs enligt artikel 6.3. Syftet med tillståndskravet och registret får anses kunna utläsas ur författningsregleringen som helhet, särskilt 10 §.

Utöver bestämmelsen i 9 § om register regleras, som nämnts, i princip inte personuppgiftsbehandling i författningen. Möjligen kan man se bestämmelsen om ansökans innehåll som en indirekt reglering av vilka personuppgifter som kommer att behandlas inom ramen för ett tillståndsärende. Detta får i så fall anses vara en tillåten precisering av personuppgiftsbehandlingen i enlighet med artikel 6.2 och 6.3 i dataskyddsförordningen.

Finns det något behov av nya kompletterande bestämmelser?

I dag gäller personuppgiftslagen för personuppgiftsbehandlingen i registret över hotell- och pensionatrörelser och i övrigt för den personuppgiftsbehandling som behövs för att handlägga ärenden om tillstånd m.m. Som redan beskrivits innehåller lagen om hotell och pensionatrörelse ingen bestämmelse som upplyser om tillämplig reglering av personuppgiftsbehandling. Lagen om hotell- och pensionatrörelse är en författning vars huvudsakliga innehåll inte avser personuppgiftsbehandling eller dataskydd. Den behöver heller inte ändras som en följd av att dataskyddsförordningen ska börja tillämpas. Som vi anförde i våra allmänna överväganden skulle det i sådana fall endast tynga författningstexten att ha med en upplysande bestämmelse om förhållandet till dataskyddsförordningen eller annan reglering av personuppgiftsbehandling. Att inleda ett lagstiftningsarbete endast för att införa en upplysande bestämmelse framstår också som omotiverat. Vi föreslår därmed ingen upplysande bestämmelse i lagen.

Inte heller har vi sett några andra skäl att införa bestämmelser avseende dataskydd i lagen om hotell- och pensionatrörelse. När det gäller behovet att inskränka den enskildes rättigheter hänvisar vi till våra allmänna överväganden, avsnitt 2.5.8.

11 Förordningen om tjänstekort

11.1 Om författningen

Förordningen (1958:272) om tjänstekort innehåller bestämmelser om utfärdande och innehav av tjänstekort. Ett tjänstekort är en särskild legitimationshandling som utfärdas för den som tjänstgör vid eller innehar uppdrag för statligt eller kommunalt organ och som regelmässigt behöver styrka sin identitet eller tjänsteställning (1 §). Vilka uppgifter som ska framgå av själva tjänstekortet anges i 4 § i förordningen.

Den bestämmelse i förordningen som har med personuppgiftsbehandling att göra är 5 §, som anger att myndigheter som utfärdar tjänstekort ska föra ett tjänstekortsregister. Registret ska innehålla bl.a. innehavarens namn och personnummer.

11.2 Överväganden

Bedömning: Behandlingen av personuppgifter i tjänstekortsregister uppfyller kraven på rättslig grund i dataskyddsförordningens artikel 6.1 och 6.3. Bestämmelsen i 5 § förordningen om tjänstekort är förenlig med dataskyddsförordningen och behöver inte ändras som en följd av att dataskyddsförordningen ska börja tillämpas. Att dataskyddsförordningen ska börja tillämpas medför inte heller att några andra ändringar eller tillägg behöver göras i förordningen om tjänstekort.

Skälen för bedömningen:

Dataskyddsförordningens krav på rättslig grund

Syftet med innehav av tjänstekort är att personal vid vissa statliga eller kommunala organ ska kunna styrka sin identitet eller sin tjänsteställning på ett betryggande sätt. Att utfärda tjänstekort är att betrakta som en uppgift av allmänt intresse. För att kunna uppnå syftet krävs att tjänstekort är tillförlitliga och att innehavet och uppgifterna på ett tjänstekort kan kontrolleras. För detta behövs ett register över tjänstekortsinnehavare. Personuppgiftsbehandlingen i tjänstekortsregister får alltså anses nödvändig för att utföra uppgiften av allmänt intresse och har därmed en rättslig grund i artikel 6.1 e dataskyddsförordningen. Att föra registret är därtill en rättslig förpliktelse (artikel 6.1 c) eftersom registret ska föras (5 § i förordningen om tjänstekort). Både uppgiften av allmänt intresse och förpliktelsen att föra registret är författningsreglerad, och kravet på att den rättsliga grunden ska vara fastställd i nationell rätt i artikel 6.3 är därmed uppfyllt. Syftet med personuppgiftsbehandlingen (som enligt artikel 6.3 ska tas in i nationell rätt vid rättsliga förpliktelser) framgår av författningen, inte minst av 1 §.

Regleringen är förenlig med dataskyddsförordningen

Den rättsliga regleringen av tjänstekortsregister utgörs av en enda paragraf i förordningen om tjänstekort. Utöver den rättsliga förpliktelsen att föra registret innehåller paragrafen bestämmelser om tjänstekortsregisters innehåll. En sådan precisering av personuppgiftsbehandlingen är tillåten i enlighet med dataskyddsförordningens artikel 6.2, se våra allmänna överväganden i avsnitt 2.5.4.

Tjänstekortsregister innehåller i enlighet med 5 § personnummer. Som framgår av våra allmänna överväganden finns en bestämmelse i dataskyddsförordningen som särskilt avser nationella identifikationsnummer – artikel 87. Av våra allmänna överväganden framgår också att det i viss mån är tveksamt vilka krav artikel 87 ställer på regleringen av personnummer. För det fall artikeln krav på skyddsåtgärder skulle anses tillämpligt på behandlingen i tjänstekortsregister, menar vi att detta krav får anses

uppfyllt. Tjänstekortsregister har ett författningsreglerat och avgränsat användningsområde. Uppgifterna i tjänstekortsregister är skyddade av sekretess.¹ Vidare är användningen av personnummer i tjänstekortsregister motiverat utifrån vikten av en säker identifiering, vilket gör regleringen förenlig med bestämmelsen i 3 kap. 13 § dataskyddslagen, som i sig är förenlig med artikel 87.

Behövs en reglering av förhållandet till dataskyddsförordningen?

Vi föreslår när det gäller andra författningar som omfattas av vårt uppdrag att det ska införas bestämmelser som klargör förhållandet till dataskyddsförordningen och dataskyddslagen. Att ha sådana bestämmelser kan vara motiverat när en författning för närvarande innehåller en bestämmelse som klargör författningens förhållande till personuppgiftslagen (1998:204) eller annars innehåller hänvisningar till personuppgiftslagen.

Förordningen om tjänstekort gäller till en mycket liten del personuppgiftsbehandling. Förordningen innehåller i dag inga hänvisningar till personuppgiftslagen. Vi anser inte att det nu finns några skäl att införa en bestämmelse som klargör förhållandet till dataskyddsförordningen.

Behov av inskränkningar avseende rättigheter i artikel 16–18 och 21?

Vi har i avsnitt 2.5.8 redogjort för dataskyddsförordningens bestämmelser om den enskildes rättigheter. Vi har inte funnit några generella skäl till att införa inskränkningar i dessa rättigheter. Det har inte heller framkommit några särskilda förhållanden när det gäller personuppgiftsbehandlingen i tjänstekortsregister som innebär att det finns anledning att göra någon annan. Till våra generella

¹ Enligt 39 kap. 3 § offentlighets- och sekretesslagen gäller sekretess i personaladministrativ verksamhet för uppgift om en enskilds personliga förhållanden, om det kan antas att den enskilde eller någon närstående till denne utsätts för våld eller lider annat allvarligt men om uppgiften röjs. För anställda på vissa myndigheter, som kan antas vara särskilt utsatta för hot och trakasserier, gäller sekretess för personnummer, bild som är underlag för tjänstekort, m.fl. uppgifter, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till denne lider men. Vilka myndigheter som omfattas av sekretessen föreskrivs av regeringen, enligt bemyndigande i 39 kap. 3 §, och framgår av 10 § offentlighets- och sekretessförordningen. Regeringen föreslår i prop. 2016/17:208 en utvidgning av detta skydd till att gälla för alla offentliganställda, se särskilt s. 14 och 54 f. i propositionen.

överväganden kan följande tilläggas. Den som blir registrerad i ett tjänstekortsregister torde vara väl införstådd med behovet att föra ett sådant register och syftet med att tjänstekort utfärdas. Det framstår inte som troligt att myndigheter som för tjänstekortsregister kommer att få invändningar om behandlingen från de registrerade. Även utan att några särskilda inskränkningar av rättigheter som annars kan åberopas av den enskilde i enlighet med artikel 16–18 och 21 torde det stå klart att behandlingen i tjänstekortsregistret har ett sådant syfte och en författningsreglering som gör behandlingen motiverad även om den enskilde invänder emot den. Det finns alltså ingen anledning införa några inskränkningar med avseende på dessa artiklar i dataskyddsförordningen.

12 Förordningen om utdrag ur folkbokföringsdatabasen i och för utredning angående brott m.m.

12.1 Om författningen

Förordningen (1967:502) om utdrag ur folkbokföringsdatabasen i och för utredning angående brott m.m. (kallas *förordningen om utdrag ur folkbokföringsdatabasen* i det följande) innehåller en paragraf med två bestämmelser. Den ena ger domstolar, åklagarmyndighet, Polismyndigheten och Säkerhetspolisen rätt att för utredning av brott få utdrag ur folkbokföringsdatabasen beträffande en viss person. Den andra bestämmelsen anger att Skatteverket utformar formulär för sådana utdrag efter samråd med Åklagarmyndigheten.

Folkbokföringsdatabasen regleras i övrigt i lagen (2001:182) om behandling av personuppgifter i Skatteverkets folkbokföringsverksamhet.

12.2 Överväganden

Bedömning: Personuppgiftsbehandling i enlighet med förordningen om utdrag ur folkbokföringsdatabasen omfattas av dataskyddsförordningens tillämpningsområde. Regleringen i förordningen om utdrag ur folkbokföringsdatabasen är förenlig med dataskyddsförordningen och behöver inte ändras som en följd av att dataskyddsförordningen ska börja tillämpas.

Skälen för bedömningen: Folkbokföringsdatabasen förs av Skatteverket och regleras, som nämnts ovan, i lagen (2001:182) om behandling av personuppgifter i Skatteverkets folkbokföringsverksamhet. Folkbokföringsdatabasen är, enligt 2 kap. 1 § i den nämnda lagen, en samling personuppgifter som med hjälp av automatiserad behandling används för de ändamål som framgår av 1 kap. 4 § i lagen, bl.a. fullgörande av underrättelseskyldighet enligt lag eller förordning (punkten 3).

Skatteverket är en myndighet som har brottsbekämpande uppgifter, men att föra folkbokföringsdatabasen kan inte anses ingå i det brottsbekämpande uppdraget. Detta, menar vi, gäller även om utlämnande ur databasen görs till myndigheter som behöver uppgifterna för utredning av brott. Den personuppgiftsbehandling som regleras i förordningen om utdrag ur folkbokföringsdatabasen omfattas alltså av dataskyddsförordningens tillämpningsområde.

Lagen om behandling av personuppgifter i Skatteverkets folkbokföringsverksamhet har ingått i en översyn inom Finansdepartementet av registerförfattningar inom departementets ansvarsområde. Överväganden finns i promemorian *EU:s dataskyddsförordning: Anpassade regler om personuppgiftsbehandling inom skatt, tull och exekution* (Fi2017/02899/S3). I promemorian görs bedömningen att lagregleringen i huvudsak är förenlig med dataskyddsförordningen och att personuppgiftsbehandlingen i enlighet med lagen uppfyller dataskyddsförordningens krav på rättslig grund i enlighet med artikel 6.1 och 6.3.¹

Författningsregleringen i förordningen om utdrag ur folkbokföringsdatabasen innebär att behandlingen för att lämna ut uppgifter till brottsbekämpande myndigheter omfattas av ändamålen för folkbokföringsdatabasen. Liksom regleringen i lagen om behandling av personuppgifter i Skatteverkets folkbokföringsverksamhet är förordningens bestämmelser förenliga med dataskyddsförordningen, oavsett om man ser regleringen som en del av den rättsliga grunden för behandlingen eller som en precisering av ändamål och utlämnande som är tillåten enligt artikel 6.2 och 6.3.

Eftersom utlämnandet enligt förordningen om utdrag ur folkbokföringsdatabasen omfattas av folkbokföringsdatabasens primära ändamål bedömer vi att ett utlämnande inte är en vidarebehandling

¹ Se särskilt s. 54 f.

för ett nytt ändamål. Det blir alltså inte nödvändigt att bedöma utlämnandets förenlighet med artikel 6.4.

Förordningen om utdrag ur folkbokföringsdatabasen kan betraktas som en komplettering till lagregleringen av folkbokföringsverksamheten. Den huvudsakliga regleringen som preciserar villkoren för behandling m.m. finns alltså i lagen om behandling av personuppgifter i Skatteverkets folkbokföringsverksamhet. I denna lag kommer att införas bl.a. en upplysande bestämmelse om dataskyddsförordningen. Det finns ingen anledning att därtill ha upplysande bestämmelser i förordningen. Frågor om behov av författningsreglering med beaktande bl.a. av den enskildes rättigheter enligt dataskyddsförordningen har bedömts inom ramen för översynen inom Finansdepartementet. Vi ser därmed ingen anledning att göra några sådana överväganden inom ramen för vårt uppdrag i denna del.

13 Efterlysningskungörelsen

13.1 Om författningen

Innehållet i kungörelsen

Efterlysning är en åtgärd som innebär att uppgifter om en eftersökt person tas in i efterlysningsregistret (2 § i kungörelsen). Förutsättningarna för att efterlysa en person framgår av 1 och 5 §§ i kungörelsen. Efterlysningsregistret innehåller också vissa andra uppgifter om beslut som har betydelse för passhindersundersökning, såsom beslut om övervakning enligt 24 kap. 4 rättegångsbalken eller beslut om förbud att utfärda pass (13 a §).

Polismyndigheten och vissa andra myndigheter beslutar om efterlysning (6 §) och ett sådant beslut ligger till grund för verkställighet av efterlysningen, dvs. införande i efterlysningsregistret. Myndigheter som inte själva kan fatta beslut om efterlysning kan i stället begära att beslut ska fattas (6 §). Framställningar om efterlysning eller om att beslut om efterlysning ska verkställas ska innehålla vissa uppgifter om den efterlyste, anledningen till efterlysningen m.m. (7 §).

Om en person förekommer i efterlysningsregistret kan det få ingripande följder, exempelvis att han eller hon nekas utresa ur riket. Efterlysningar som inte längre är aktuella av olika anledningar ska därför genast återkallas och registreringen av personen i efterlysningsregistret tas bort (9 §). Vissa efterlysningar gäller endast under ett år, varefter ett nytt beslut om efterlysning ska fattas eller registreringen i efterlysningsregistret tas bort (12 §).

Förhållandet till annan lagstiftning

Efterlysningkungörelsen innehåller inte någon bestämmelse som uttryckligen reglerar förhållandet till andra författningar om personuppgiftsbehandling. Av kungörelsens innehåll framgår klart att behandling av personuppgifter i efterlysningsregistret kan ske i syfte att bekämpa brott. Sådan personuppgiftsbehandling inom Polismyndigheten omfattas annars av polisdatalagens (2010:361) reglering. Eftersom efterlysningkungörelsen inte undantas från polisdatalagens tillämpningsområde omfattas även personuppgiftsbehandlingen i registret av polisdatalagen, så länge den kan anses ske för de syften som avgränsar lagens tillämpningsområde.¹

Frågan är dock om all personuppgiftsbehandling i efterlysningsregistret kan anses ske i brottsbekämpande syfte.

Datainspektionen har i ett beslut kommit fram till att behandling av uppgifter om efterlysta personer inte i alla sammanhang kan anses ske för syften som omfattas av polisdatalagens tillämpningsområde. Beslutet gällde uppgifter i polisens s.k. OBS-portal, ett informationssystem som innehåller gemensamt tillgängliga uppgifter i enlighet med polisdatalagen. I portalen hade publicerats uppgifter om personer som var efterlysta för att de avvikit från olika former av tvångsvård. Polismyndigheten menade att personuppgiftsbehandlingen skulle anses hänförlig till polisens verksamhet med att förebygga brott, eftersom det typiskt sett finns risk för att personer som avviker från pågående vårdinsatser, exempelvis unga och missbrukare, kan hamna i kriminella miljöer och antingen begå brott eller själva bli utsatta för brott. Datainspektionen var dock av motsatt uppfattning och menade att i vart fall den aktuella personuppgiftsbehandlingen inte kunde hänföras till förebyggande av brott, eftersom det inte fanns någon information som visade att de efterlysta personerna hade någon koppling till brottslig verksamhet.² Det kan tilläggas att Datainspektionen hänvisade till polisdatalagens förarbeten som grund för sin slutsats i ärendet. I propositionen tas inte specifikt upp frågan om efterlysta personer. Däremot nämns att personuppgiftsbehandling med anledning av polisens uppgift med vissa verkställighetsåtgärder på kriminal-

¹ Se t.ex. JK Dnr 1570-15-42.

² Datainspektionens beslut 2016-04-18, dnr 211-2015.

vårdens och socialtjänstens område inte har till syfte att bekämpa brott i egentlig mening och därmed inte omfattas av polisdatalagens tillämpningsområde.³

I RÅ 1988 not 776 uttalas att efterlysning av personer som anmälts som försvunna ska bedömas som polisiär verksamhet för att ge hjälp och bistånd till enskilda. Sådan verksamhet hör inte till vad som enligt polisdatalagen är verksamhet för att förebygga, förhindra eller upptäcka brottslig verksamhet.⁴

Om personuppgiftsbehandlingen i efterlysningsregistret i vissa fall inte går att inordna under polisdatalagens tillämpningsområde innebär det att personuppgiftslagen i stället gäller för sådan behandling.

13.2 Överväganden

Bedömning: Behandlingen av personuppgifter i enlighet med efterlysningkungörelsen omfattas antingen av det nya dataskyddsdirektivets eller dataskyddsförordningens tillämpningsområde, beroende på syftet med behandlingen.

Det behövs inga tillägg eller förändringar i efterlysningkungörelsen p.g.a. det nya dataskyddsdirektivets genomförande i nationell rätt eller som en följd av att dataskyddsförordningen ska börja tillämpas.

Skälen för bedömningen:

Vilken EU-rättsakt är tillämplig?

Efterlysningsregistret är ett automatiserat system för behandling av personuppgifter. Behandlingen i registret är därmed en sådan personuppgiftsbehandling som omfattas antingen av dataskyddsförordningens eller det nya dataskyddsdirektivets tillämpningsområde.

Det står klart att vissa efterlysningar har till syfte att bekämpa brott eller verkställa straffrättsliga påföljder, exempelvis då det

³ Prop. 2009/10:85 s. 74 f.

⁴ A. prop. s. 75.

gäller efterlysningar av misstänkta personer eller personer som avvikit från verkställigheten av frihetsberövande straff.

I andra fall kan det diskuteras i vilket syfte personuppgifterna behandlas. Frågan har inte tagits upp av Utredningen om 2016 års dataskyddsdirektiv. Utredningen har dock anfört att uttrycket *förebygga, förhindra och upptäcka brottslig verksamhet*, som används i brottsdatalagen, ska ges samma innebörd som uttrycket har när det används i nuvarande registerförfattningar för de berörda myndigheterna.⁵ Av intresse i sammanhanget är därmed tidigare uttalanden om syftet med att behandla uppgifter om efterlysta personer och om sådan behandling omfattas av polisdatalagen. Som vi redogjort för ovan finns uttalanden som talar för att personuppgiftsbehandlingen avseende försvunna personer inte alltid sker i brottsbekämpande syfte. Med andra ord kan personuppgiftsbehandlingen i sådana fall knappast inordnas under det nya dataskyddsdirektivets eller brottsdatalagens tillämpningsområde avseende att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott. Att eftersöka försvunna personer kan i allmänhet inte heller hänföras till verksamhet som syftar till att upprätthålla allmän ordning och säkerhet, i vart fall inte med den tolkning av det nya dataskyddsdirektivet i denna del som Utredningen om 2016 års dataskyddsdirektiv förordar. Att kommissionen har ansett att personuppgiftsbehandlingen i SIS kan omfattas både av det nya dataskyddsdirektivet och av dataskyddsförordningen har också betydelse i sammanhanget, även om det givetvis får beaktas att bedömningen för närvarande framkommer i ett förslag och att det inte är närmare specificerat vilka behandlingar som anses falla inom dataskyddsförordningens tillämpningsområde.

Vi vill återigen (jfr avsnitt 5.2) framhålla att frågan om gränsdragningen mellan dataskyddsförordningens tillämpningsområde och det nya dataskyddsdirektivet i vissa fall är svår att göra och att det inte är uteslutet att man skulle kunna ha en något vidare syn på vad som omfattas av att exempelvis förebygga och förhindra brottslig verksamhet i direktivets mening än den vi redovisat ovan. För att ge ett så brett beredningsunderlag som möjligt menar vi dock att vi får utgå ifrån att det, på samma sätt som när det gäller

⁵ SOU 2017:29 s. 161 f.

personuppgiftsbehandlingen i SIS, får bedömas från fall till fall om personuppgiftsbehandlingen i efterlysningsregistret och vid handläggningen av ett ärende om efterlysning omfattas av dataskyddsförordningen eller det nya dataskyddsdirektivet. Efterlysningkungörelsen är därmed en författning som får analyseras både i förhållande till det nya dataskyddsdirektivet och dataskyddsförordningen.

Överväganden i förhållande till dataskyddsförordningen

Att föra efterlysningsregistret kan betraktas både som en rättslig förpliktelse för Polismyndigheten och som en personuppgiftsbehandling som är nödvändig för att utföra en uppgift av allmänt intresse (artikel 6.1 c respektive e). Författningsregleringen av förutsättningarna för efterlysning och införande i registret innebär att den rättsliga grunden är fastställd på sätt som krävs enligt artikel 6.3. Det kan anmärkas att det övergripande syftet med personuppgiftsbehandlingen framgår av författningsregleringen – syftet är att underlätta eftersökningen av personer som det saknas uppgifter om var de befinner sig (1 §).

Efterlysningkungörelsen preciserar i övrigt vilka uppgifter om en person som ska ingå i en framställning om efterlysning (7 §). I den mån framställningar innebär en automatiserad behandling av personuppgifterna utgör regleringen en precisering som är förenlig med dataskyddsförordningen i enlighet med artikel 6.2 och 6.3.

Slutligen innehåller efterlysningkungörelsen bestämmelser om radering ur registret (9 och 12 §§). Även om bestämmelserna kan anses ge uttryck för den allmänna principen att personuppgifter inte ska bevaras längre än vad som behövs för ändamålet med behandlingen, innebär bestämmelserna särskilda förfaranderegler som preciserar under vilka förutsättningar och på vilket sätt behandlingen av personuppgifter ska upphöra. Bestämmelserna kan därmed inte anses endast upprepa vad som annars sägs i dataskyddsförordningen och de behöver därmed inte ändras för att förordningen ska börja tillämpas.

Överväganden i förhållande till det nya dataskyddsdirektivet

Även i förhållande till det nya dataskyddsdirektivet utgör efterlysningkungörelsen en sådan rättslig grund som gör personuppgiftsbehandlingen i registret laglig. De övriga preciseringarna av personuppgiftsbehandlingen är förenliga med det nya dataskyddsdirektivet (jfr våra allmänna överväganden, avsnitt 2.6.2 och 2.6.3).

Behövs nya bestämmelser i efterlysningkungörelsen?

Efterlysningkungörelsen gäller för närvarande utöver personuppgiftslagen, utom i de fall då personuppgifter behandlas inom ramen för polisdatalagens tillämpningsområde. Detta framgår dock inte av författningen i sig, vare sig i någon upplysande bestämmelse eller i övrigt genom hänvisningar till personuppgiftslagen. Som vi utvecklar i det följande kommer vi inte att föreslå några ändringar i efterlysningkungörelsen som en följd av någon av EU-rättsakterna. Efterlysningkungörelsen är därtill en författning som inte i huvudsak reglerar frågor om dataskydd, utan som innehåller en reglering av polisens uppgift att hantera efterlysningar och förfarandet för att utfärda efterlysning. Som vi anfört i våra allmänna överväganden finns det för sådana författningar ett mindre behov av att införa upplysande bestämmelser som hänvisar till övergripande dataskyddsreglering. Sammantaget menar vi alltså att några upplysande bestämmelser om personuppgiftsbehandling inte behövs i efterlysningkungörelsen.

När dataskyddsförordningen ska börja tillämpas och brottsdatalagen med tillhörande registerförfattningar träder i kraft, kommer efterlysningkungörelsen att utgöra en kompletterande författningsreglering i förhållande till dessa regelverk i stället för till personuppgiftslagen. Samma förhållande till polisens brottsdatalag som det nuvarande förhållandet till polisdatalagen kommer att gälla, dvs. polisens brottsdatalag kommer att vara tillämplig på uppgifter som förs in i efterlysningsregistret i den mån införandet i registret behövs för något av de syften som utgör rättsliga grunder enligt polisens brottsdatalag.⁶

⁶ Se vidare SOU 2017:74 s. 96.

Som tidigare redogjorts för innebär dataskyddsförordningen vissa särregler när det gäller uppgifter om lagöverträdelse, personnummer och känsliga personuppgifter. Att personnummer förekommer i efterlysningsregistret är självklart för att undvika personförväxlingar. Användandet av personnummer regleras dock inte i efterlysningsskugörelsen och därmed kommer 3 kap. 13 § dataskyddslagen vara tillämplig för sådan behandling som omfattas av dataskyddsförordningens tillämpningsområde.

Efterlysningsregistret kan typiskt sett innehålla både känsliga personuppgifter⁷ och uppgifter om fällande domar i brottmål. Uppgifter om domar i brottmål torde i och för sig bli aktuella endast då en efterlysning syftar till att bekämpa brott eller verkställa straffrättsliga påföljder. Förutsättningarna att behandla sådana uppgifter är annars uppfyllda även inom dataskyddsförordningens tillämpningsområde eftersom efterlysningsregistret förs av en myndighet (se artikel 10). Att behandla känsliga personuppgifter avseende efterlysta personer, exempelvis avseende hälsa (personer som tvångsvårdas), torde vara absolut nödvändigt för ändamålet med behandlingen i enlighet med 3 kap. 3 § dataskyddslagen.

Inom det nya dataskyddsdirektivets tillämpningsområde kommer personuppgiftsbehandling, som redan redogjorts för, att omfattas av både brottsdatalagen och polisens brottsdatalag. Behandlingen av känsliga personuppgifter och sökbegränsningar gällande sådana uppgifter kommer att regleras av dessa båda lagar. Att känsliga personuppgifter kan komma att behandlas i efterlysningsregistret torde vara förenligt med 2 kap. 11 § brottsdatalagen.

När det gäller den enskildes rättigheter i dataskyddsförordningen har vi i våra allmänna överväganden (se avsnitt 2.5.8) kommit fram till att det inte finns några generella skäl att inskränka rättigheterna. Vi har heller inte funnit några argument för en annan bedömning som särskilt skulle gälla för personuppgiftsbehandlingen i efterlysningsregistret. Eftersom förutsättningarna för efterlysning klart framgår av författningen bör felaktigheter i registret tämligen lätt kunna utredas och leda till att en felaktig efterlysning genast tas bort utan att det ska behöva bli frågan om att utreda förutsättningarna för exempelvis begränsning av behandlingen eller liknande.

⁷ Jfr prop. 2009/10:85 s. 470.

När det gäller skadestånd finns ingen hänvisning till personuppgiftslagens reglering av skadestånd i efterlysningkungörelsen. Som vi tidigare anført anser vi att det inte behövs några hänvisningar till dataskyddsförordningen för att den enskilde ska ha möjlighet att kräva skadestånd enligt förordningen. Eftersom behandling av personuppgifter i efterlysningsregistret inom det brottsbekämpande området kommer att ske inom ramen för den föreslagna polisens brottsdatalag, kommer rätten till skadestånd för den enskilde att bedömas i enlighet med denna lag⁸.

Som vi tidigare anført (se avsnitt 2.5.9) finns ingen anledning att särskilt hänvisa till systemet med sanktionsavgifter avseende personuppgiftsbehandling inom dataskyddsförordningens tillämpningsområde. Utredningen om 2016 års dataskyddsdirektiv föreslår däremot hänvisningar till brottsdatalagen avseende sanktionsavgifter i registerförfattningar inom brottsdatalagens tillämpningsområde. Vi har däremot bedömt att det inte finns behov att införa några sådana hänvisningar i registerförfattningar som omfattas av vårt uppdrag, se våra allmänna överväganden, avsnitt 2.6.7.

⁸ Jfr återigen det redan nämnda JK-beslutet, dnr 1570-15-42.

14 Ikraftträdande och övergångsbestämmelser

14.1 Författningsförslag inom dataskyddsförordningens tillämpningsområde

Förslag: Kustbevakningsdatalagen och kustbevakningsdataförordningen ska träda i kraft den 25 maj 2018. Även ändringar i vapenlagen och förordningen om införsel av farliga föremål ska träda ikraft den 25 maj 2018. Detsamma gäller de huvudsakliga ändringarna i förordningen om uppdragsverksamhet vid NFC. Ändringen i den förordningen som följer av att polisdatalagen ändrar namn till polisens brottsdatalag ska dock träda i kraft den 1 maj 2018.

Bedömning: Övergångsbestämmelser behövs inte.

Skälen för förslaget och bedömningen: Dataskyddsförordningen ska börja tillämpas den 25 maj 2018. Författningsförslag som föranleds av att förordningen ska börja tillämpas bör därför träda i kraft samma dag. Även dataskyddslagen kommer att träda i kraft den 25 maj 2018. Dataskyddsutredningen har föreslagit vissa övergångsbestämmelser till dataskyddslagen som rör bl.a. tillsynsärenden och överklagande. För eventuella tillsynsärenden m.m. som rör personuppgiftsbehandling enligt de författningar där vi föreslår ändringar blir alltså övergångsbestämmelserna till dataskyddslagen tillämpliga. Det kan anmärkas att det följer av allmänna rättsgrundsatser att äldre bestämmelser om skadestånd gäller för skada som orsakats före ikraftträdandet av en ny reglering. Dataskyddslagen innehåller därtill en uttrycklig övergångs-

bestämmelse av samma innebörd. Några övergångsbestämmelser till våra författningsförslag behövs alltså inte i något avseende.

Även när det gäller vårt förslag till kustbevakningsdatalag och kustbevakningsdataförordning gör vi bedömningen att författningarna kan börja tillämpas när de träder i kraft utan övergångsbestämmelser. I kustbevakningsdatalagen hänvisas till Kustbevakningens brottsdatalag. Kustbevakningens brottsdatalag är det föreslagna namnet på den nu gällande kustbevakningsdatalagen. Vi utgår ifrån att lagstiftningsarbetet samordnas så att författningsändringarna i den nu gällande kustbevakningsdatalagen i vart fall kommer att träda i kraft senast vid samma tidpunkt som den nya kustbevakningsdatalag som vi föreslår. Därmed föranleder inte heller hänvisningen till Kustbevakningens brottsdatalag några förslag till övergångsbestämmelser från vår sida. Det kan anmärkas att om Kustbevakningens brottsdatalag ska träda i kraft tidigare än den 25 maj 2018 finns behov av övergångsbestämmelser i den lagen. Utredningen om 2016 års dataskyddsdirektiv har redogjort för hur sådana övergångsbestämmelser kan utformas om de skulle behövas.¹

14.2 Författningsförslag inom det nya dataskyddsdirektivets tillämpningsområde

Förslag: Förslaget till ändring i förordningen om förenklat uppgiftsutbyte mellan brottsbekämpande myndigheter i Europeiska unionen ska träda ikraft den 1 maj 2018.

Skälen för förslaget: Vårt förslag till ändring i förordningen om förenklat uppgiftsutbyte föranleds av att lagen (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polis-samarbete och straffrättsligt samarbete inom Europeiska unionen kommer att upphöra att gälla. Författningsändringen bör därför träda ikraft samma dag som upphävandet av den lagen, alltså den 1 maj 2018.²

¹ SOU 2017:74 s. 764–766.

² 2013 års lag upphävs genom brottsdatalagen, se SOU 2017:29 s. 56.

14.3 Författningsförslag inom både det nya dataskyddsdirektivets och dataskyddsförordningens tillämpningsområde

Förslag: Ändringar i bestämmelser som avser personuppgiftsbehandling inom det nya dataskyddsdirektivets tillämpningsområde bör träda i kraft samma dag som brottsdatalagen, således den 1 maj 2018. Det gäller ändringar i lagen om belastningsregister, lagen om misstankeregister och lagen om Schengens informationssystem. Införandet av bestämmelser i dessa författningar som avser att upplysa om tillämpningen av dataskyddsförordningen och dataskyddslagen ska i stället träda i kraft den 25 maj 2018. Lagarna i sin lydelse före den 1 maj 2018 ska fortsätta vara tillämpliga fram till den 25 maj 2018 på personuppgiftsbehandling som inte omfattas av brottsdatalagens tillämpningsområde.

Ändringarna i förordningen om Schengens informationssystem ska träda ikraft den 1 maj 2018.

Bedömning: Några övergångsbestämmelser i övrigt behövs inte.

Skälen för förslaget och bedömningen: Vissa författningar som ingår i vår översyn reglerar personuppgiftsbehandling som omfattas antingen av det nya dataskyddsdirektivet eller av dataskyddsförordningen. Det gäller lagen och förordningen om Schengens informationssystem, lagen och förordningen om belastningsregister samt lagen och förordningen om misstankeregister.

För att det nya dataskyddsdirektivet ska bli korrekt genomfört avseende den personuppgiftsbehandling som sker inom direktivets tillämpningsområde bör ändringar i författningarna som hänvisar till brottsdatalagen och som i övrigt beror av att brottsdatalagen ska börja tillämpas träda ikraft samtidigt som denna lag, dvs. den 1 maj 2018. Dataskyddsförordningen och dataskyddslagen kommer dock inte att börja tillämpas förrän den 25 maj 2018. Bestämmelser som upplyser om att dessa regelverk ska tillämpas för viss personuppgiftsbehandling enligt registerförfattningarna kan därmed inte träda ikraft förrän den 25 maj 2018. För personuppgiftsbehandlingen inom dataskyddsförordningens tillämpnings-

område kan andra ändringar i författningarna inte heller börja tillämpas förrän den 25 maj 2018. Det gäller ändringarna i lagen om belastningsregister och lagen om misstankeregister som innebär att hänvisningen till bestämmelser om skadestånd och rättelse m.m. i personuppgiftslagen tas bort. Det gäller vidare upphävandet av bestämmelser om rättelse m.m. i lagen om SIS. Om dessa ändringar skulle träda i kraft före det att dataskyddsförordningen ska börja tillämpas, skulle personuppgiftsbehandling som inte omfattas av brottsdatalagen sakna tillämpliga bestämmelser om rättelse och skadestånd. För sådan personuppgiftsbehandling måste alltså lagarnas lydelse före den 1 maj 2018 tillämpas fram till dess dataskyddsförordningen träder in som det generella regelverket och personuppgiftslagen upphör att gälla, alltså den 25 maj 2018. Övergångsbestämmelser av denna innebörd behövs därmed i de nämnda lagarna.

När det gäller ändringarna i förordningen om Schengens informationssystem har dessa utformats så att de inte innehåller några hänvisningar till andra lagar. De kan alltså tillämpas oberoende av vilket generellt regelverk som ska tillämpas. Ändringarna kan därmed träda ikraft den 1 maj 2018.

Vi bedömer att inga andra övergångsbestämmelser än dem vi redogjort för ovan behövs, i enlighet med vad vi anført i föregående avsnitt. Det kan anmärkas att brottsdatalagen, liksom dataskyddslagen, innehåller en uttrycklig övergångsbestämmelse avseende skadestånd. Övergångsbestämmelsen i brottsdatalagen är utformad så att den torde omfatta även skadestånd för personuppgiftsbehandling som utförts i enlighet med en registerförfattning inom brottsdatalagens tillämpningsområde.

15 Konsekvenser

Bedömning: Förslagen kan medföra vissa administrativa kostnader för berörda myndigheter, framför allt initialt för att myndigheterna ska sätta sig in i den nya regleringens utformning och struktur. Sådana kostnader ryms inom befintliga anslag. Förslagen innebär inte i sig något förstärkt skydd för den personliga integriteten, utan möjliga sådana konsekvenser följer av de nya generella regelverken och deras tillämpning. Förslagen får i huvudsak inga konsekvenser för brottsbekämpningen eller övrig berörd verksamhet.

Skälen för bedömningen:

Vårt uppdrag när det gäller konsekvensbedömningar

Enligt vår uppdragsbeskrivning (se bilaga 1) ska vi analysera och redovisa våra förslags

- ekonomiska konsekvenser
- konsekvenser för den personliga integriteten
- konsekvenser för brottsbekämpningen och övrig berörd verksamhet

Om kostnader bedöms uppkomma ska ett finansieringsförslag lämnas.

Ekonomiska konsekvenser

Till övervägande del innebär våra förslag i sig inga förändringar som påverkar de materiella förutsättningarna för de berörda myndigheternas behandling av personuppgifter. I stället avser våra förslag

huvudsakligen upplysande bestämmelser och hänvisningar till annan reglering av personuppgiftsbehandling. Huruvida dessa generella regelverk ställer krav på myndigheternas personuppgiftsbehandling eller i övrigt förändrar de materiella förutsättningarna på något sätt som medför kostnader för verksamheten är en fråga som vi menar ligger utanför vårt uppdrag. I de fall våra förslag innebär materiella förändringar (exempelvis avseende möjligheterna att lämna ut personuppgifter elektroniskt, se avsnitt 3.5.5) ställs det inga nya krav på myndigheterna, utan avsikten har varit att möjliggöra en förenkling och effektivisering i verksamheten.

Även om våra förslag således inte medför några krav på förändringar av själva personuppgiftsbehandlingen krävs givetvis en viss anpassning hos myndigheterna, framför allt för att sätta sig in i den nya regleringens utformning och struktur. Den största förändringen för de myndigheter som berörs av våra förslag bedömer vi dock vara de nya generella regelverken. En särskild komplikation för myndigheterna blir att hantera det faktum att personuppgiftslagen ersätts av tre nya generella regelverk – brottsdatalagen, dataskyddsförordningen och dataskyddslagen. Enligt vår bedömning är det detta förhållande som kommer att skapa de största administrativa kostnaderna för myndigheterna när det gäller anpassning till den nya rättsliga miljön. Med beaktande av detta går det knappast att särskilja eller bedöma de kostnader som kan uppkomma som en följd av våra förslag, annat än att de torde vara marginella i sammanhanget. Under alla förhållanden gör vi bedömningen att de i sig ryms inom befintliga anslag.

Konsekvenser för den personliga integriteten

Avsikten med EU:s dataskyddsreform är att stärka skyddet av den personliga integriteten vid behandling av personuppgifter. I den mån några sådana effekter kan uppnås beror detta på de allmänna bestämmelserna om personuppgiftsbehandling som finns i den generella regleringen, såsom den enskildes rättigheter till information, invändningar och begränsningar, möjligheten till skadestånd, tillsyn m.m. Dessa bestämmelser skulle, med något enstaka undantag, ha kunnat tillämpas även utan de författningsändringar vi föreslår. Vi menar därför att våra förslag inte i sig kan sägas få några konsekvenser för den personliga integriteten.

Konsekvenser i övrigt för de berörda myndigheternas verksamhet

Eftersom våra förslag i sig inte innebär några materiella förändringar kommer de inte att innebära några konsekvenser för de berörda myndigheternas verksamhet, inklusive brottsbekämpning. Myndigheterna har alltså, endast med beaktande av våra förslag, samma möjligheter som tidigare att behandla personuppgifter i de verksamheter som berörs av förslagen.

Sammanfattning

Sammanfattningsvis menar vi att våra förslag inte för med sig annat än i sammanhanget marginella kostnader för de berörda myndigheterna och att dessa ryms inom befintliga anslag. Kostnaderna avser initiala administrativa kostnader för att myndigheterna ska kunna sätta sig in i den nya regleringens utformning och struktur. Vi bedömer inte att våra förslag får några andra konsekvenser.

16 Författningskommentar

16.1 Förslaget till kustbevakningsdatalag

Lagen är ny, men innehållet motsvarar i stora delar innehållet i 1, 2 och 5 kap. kustbevakningsdatalagen (2012:145) i den utformning lagen hade före genomförandet av det nya dataskyddsdirektivet (kallas *2012 års kustbevakningsdatalag* i det följande). Genomförandet av direktivet har medfört att 2012 års kustbevakningsdatalag har fått ett delvis nytt innehåll samt ett nytt namn, Kustbevakningens brottsdatalag. Bestämmelser som i 2012 års kustbevakningsdatalag avsåg myndighetens brottsbekämpande verksamhet (3 och 4 kap.) har anpassats och ändrats i den omfattning som har motiverats av genomförandet av det nya dataskyddsdirektivet och införandet av brottsdatalagen (2018:00), se vidare SOU 2017:74. I förevarande lag finns i stället de bestämmelser som reglerar Kustbevakningens personuppgiftsbehandling inom dataskyddsförordningens tillämpningsområde.

I förhållande till 1, 2 och 5 kap. i 2012 års kustbevakningsdatalag har paragraferna delvis en ny inbördes placering och lagen är inte längre kapitelindelad. Med hänsyn till detta har några nya rubriker tillkommit och vissa andra har utgått. Dessa förändringar är endast redaktionella och avser inte att göra någon saklig skillnad vid tillämpningen.

1 §

Paragrafen anger lagens syfte. Den motsvarar 1 kap. 1 § i 2012 års kustbevakningsdatalag. Överväganden finns i avsnitt 3.5.1. För en kommentar till paragrafen, se prop. 2011/12:45 s. 191.

2 §

Paragrafen anger lagens tillämpningsområde. Överväganden finns i avsnitt 3.5.1.

Paragrafens *första stycke* motsvarar i huvudsak 1 kap. 2 § första stycket i 2012 års kustbevakningsdatalag. Skillnaden är att första punkten i den bestämmelsen – *brottsbekämpning* – har utgått. Personuppgiftsbehandling som behövs för Kustbevakningens brottsbekämpande verksamhet regleras i stället av Kustbevakningens brottsdatalag, vilket framgår av *andra stycket*. Kustbevakningens brottsdatalag reglerar också personuppgiftsbehandling i syfte att upprätthålla allmän ordning och säkerhet. I sak avser förevarande kustbevakningsdatalags uttryck *sjöövervakning* samma verksamhet som 2012 års kustbevakningsdatalag, med undantag för sjöövervakning som syftar till att upprätthålla allmän ordning och säkerhet (jfr prop. 2011/12:45 s. 157 och s. 220). En utförligare redogörelse av vad som avses med upprätthållande av allmän ordning och säkerhet när det gäller Kustbevakningens verksamhet finns i *Brottsdatalag – kompletterande lagstiftning* (SOU 2017:74 s. 475–478 och 904) och i övervägandena till förevarande paragraf, avsnitt 3.5.1.

Liksom tidigare gäller att tillämpningsområdet för lagen endast omfattar de angivna delarna av den operativa verksamheten. Behandling som rör interna och administrativa åtgärder inom myndigheten, exempelvis i personal- och löneregister, omfattas inte av lagen (a. prop. s. 191). Tidigare gällde personuppgiftslagen för sådan behandling, men i och med upphävandet av personuppgiftslagen tillämpas i stället dataskyddsförordningen och dataskyddslagen, se vidare kommentaren till 3 och 4 §§.

Av *tredje stycket* framgår att endast helt eller delvis automatiserad behandling eller behandling i en strukturerad samling av personuppgifter som är tillgänglig för sökning eller sammanställning enligt särskilda kriterier. Begreppet *personuppgifter* definieras i dataskyddsförordningen. Helt manuell behandling av personuppgifter som inte heller ingår i en sådan strukturerad samling som anges i bestämmelsen, omfattas inte av lagen (a. prop. s. 191).

3 §

Paragrafen upplyser om att lagen innehåller bestämmelser som kompletterar dataskyddsförordningen. Överväganden finns i avsnitt 3.5.4.

Dataskyddsförordningen utgör den generella regleringen av personuppgiftsbehandling inom sitt tillämpningsområde, inom vilket förevarande lag alltså faller. Lagens bestämmelser utgör preciseringar av dataskyddsförordningens principer för behandling i flera avseenden. Dataskyddsförordningen tillämpas i övrigt direkt på personuppgiftsbehandlingen enligt lagen.

4 §

Paragrafen upplyser om att dataskyddslagen gäller vid personuppgiftsbehandling enligt kustbevakningsdatalagen. Överväganden finns i avsnitt 3.5.4.

Inte alla bestämmelser i dataskyddslagen kommer att vara aktuella att tillämpa på Kustbevakningens personuppgiftsbehandling. Exempelvis föranleder inte regleringen av rättslig grund i 2 kap. dataskyddslagen att någon ytterligare prövning av de rättsliga förutsättningarna för Kustbevakningens personuppgiftsbehandling måste göras, så länge personuppgiftsbehandlingen utförs i enlighet med kustbevakningsdatalagen. Personuppgiftsbehandlingen enligt lagen uppfyller kraven på rättslig grund enligt dataskyddsförordningen. Överväganden om detta finns i avsnitt 3.4. Kustbevakningsdatalagen innehåller vidare avvikelser från dataskyddslagen när det gäller känsliga personuppgifter, 12 och 13 §§. Dataskyddslagen är subsidiär till annan författning, vilket framgår både av 2 § i den lagen och av bestämmelsen i förevarande lag, som anger att dataskyddslagen gäller om inte annat följer av kustbevakningsdatalagen, eller av föreskrifter som meddelats med stöd av den. Bestämmelserna i 12 och 13 §§ tillämpas alltså i stället för regleringen i 3 kap. 3 och 4 §§ dataskyddslagen.

5 §

Paragrafen anger vilka bestämmelser i lagen som också ska tillämpas på juridiska personer. Överväganden finns i avsnitt 3.5.1. Paragrafen överensstämmer i sak med 1 kap. 3 § i 2012 års kustbevakningsdatalag, se vidare a. prop. s. 192. Hänvisningarna till 3 och 4 kap. i den lagen har dock ingen motsvarighet i bestämmelsen, eftersom kustbevakningsdatalagen inte längre omfattar brottsbekämpning m.m. (se kommentaren till 2 § ovan).

6 §

Paragrafen anger att Kustbevakningen är personuppgiftsansvarig. Den har samma utformning och innebörd som 2 kap. 4 § i 2012 års kustbevakningsdatalag. Överväganden finns i avsnitt 3.5.1.

Definitionen av vad personuppgiftsansvar innebär framgår av artikel 4 i dataskyddsförordningen och inte, som tidigare, av personuppgiftslagens definition. Detta gör ingen saklig skillnad för personuppgiftsansvarets omfattning eller innebörd såvitt avser tillämpningen av de bestämmelser som finns i förevarande lag. Se vidare a. prop. s. 198 f. I den mån dataskyddsförordningen ställer andra krav på den personuppgiftsansvarige än den tidigare personuppgiftslagen, är sådana skyldigheter direkt tillämpliga för Kustbevakningen.

7–10 §§

Paragraferna reglerar primära och sekundära ändamål för behandlingen av personuppgifter. De överensstämmer i huvudsak med 5 kap. 1 och 2 §§ och 2 kap. 6 § i 2012 års kustbevakningsdatalag. Överväganden finns i avsnitt 3.5.1 och 3.5.3. Bestämmelsen i 5 kap. 1 § andra stycket i 2012 års kustbevakningsdatalag om gemensamt tillgängliga uppgifter har överförs till 15 §. Bestämmelsen i 5 kap. 2 § tredje stycket har ersatts av 11 §, se vidare kommentaren till denna paragraf.

För en kommentar till 7 och 9–10 §§ hänvisas till a. prop. s. 219–222 och för en kommentar till 8 § till a. prop. s. 199 f.

11 §

Paragrafen innehåller en hänvisning till den s.k. finalitetsprincipen. Överväganden finns i avsnitt 3.4 och 3.5.3. Paragrafen avser, liksom den tidigare bestämmelsen i 5 kap. 2 § tredje stycket i 2012 års kustbevakningsdatalag, att tydliggöra att de sekundära ändamålen (i 9 § förevarande lag) inte är uttömmande angivna. I enskilda fall kan därmed personuppgifter behandlas för att lämna information under förutsättning att ändamålet för en sådan behandling inte är oförenligt med det ändamål för vilket uppgifterna ursprungligen behandlades. Jfr a. prop. s. 222. Vid bedömningen av om ett nytt ändamål är förenligt med det ursprungliga ändamålet för behandling tillämpas finalitetsprincipen såsom den kommer till uttryck i artikel 5.1 b och artikel 6.4 i dataskyddsförordningen. Om information lämnas efter beaktande av de omständigheter som anges i artikel 6.4 a–e följer av dataskyddsförordningens skäl 50 att en sådan vidarebehandling inte behöver ha någon ytterligare rättslig grund i enlighet med artikel 6.1.

Informationslämnande till myndigheter som sker i enlighet med lag företas däremot med stöd av 9 §. Ett exempel på en sådan vidarebehandling är lämnande av uppgifter i enlighet med 6 kap. 5 § offentlighets- och sekretesslagen (jfr a. prop. s. 165).

12 §

Paragrafen avser behandling av s.k. känsliga personuppgifter. Överväganden finns i avsnitt 3.5.4.

I *första stycket* anges att känsliga personuppgifter inte får behandlas och vad som avses med begreppet. Detta görs genom en hänvisning till den uppräkningslista som finns i artikel 9.1 i dataskyddsförordningen. I dataskyddsförordningen används dock begreppet *särskilda kategorier av personuppgifter*, men någon saklig skillnad i förhållande till regleringen i paragrafen är inte avsedd. Det nya dataskyddsdirektivet och brottsdatalagen innehåller samma uppräkningslista av vissa personuppgifter som ska ingå i kategorin *känsliga personuppgifter*. I dataskyddslagen hänvisas i stället till artikel 9.1 i dataskyddsförordningen (3 kap. 1 §).

Även 1995 års dataskyddsdirektiv och personuppgiftslagen innehöll en särreglering av vissa personuppgifter som nästan helt

överensstämmer med de nu särreglerade kategorierna. Ledning för vilka personuppgifter som nu ska anses som känsliga personuppgifter kan alltså fås även från tidigare förarbeten.

I *andra stycket* anges att om personuppgifter redan behandlas på en annan grund, får de kompletteras med känsliga personuppgifter om detta är absolut nödvändigt för ändamålet med behandlingen. Denna bestämmelse överensstämmer med 2 kap. 11 § andra stycket brottsdatalagen. En kommentar till vad som ska anses vara *absolut nödvändigt* för ändamålet med behandlingen följer av SOU 2017:29 s. 691 f. Även i dataskyddslagen används uttryckssättet *absolut nödvändigt för ändamålet med behandlingen*, se vidare SOU 2017:39 s. 177 f.

I *tredje stycket* anges krav på hur uppgifter som beskriver en persons utseende ska utformas. Bestämmelsen motsvarar både 2 kap. 7 § tredje stycket i 2012 års kustbevakningsdatalag, se vidare a. prop. s. 201, och 2 kap. 7 § andra stycket brottsdatalagen, se vidare SOU 2017:29 s. 687.

13 §

I paragrafens *första stycke* finns ett sökförbud beträffande känsliga personuppgifter som överensstämmer med 2 kap. 14 § brottsdatalagen, se vidare SOU 2017:29 s. 693. Överväganden finns i avsnitt 3.5.4.

Tillämpningen av bestämmelsen är avsedd att vara i enlighet med nämnda bestämmelse i brottsdatalagen. I 2012 års kustbevakningsdatalag fanns ett motsvarande sökförbud i 5 kap. 4 §. I den paragrafen angavs i *andra stycket* att uppgifter som beskriver en persons utseende kan användas som sökbegrepp. Bestämmelsen har överförts till förevarande paragrafs *andra stycke*. För en kommentar, se a. prop. s. 223.

14 och 15 §§

Paragraferna avser förutsättningarna för behandling av *gemensamt tillgängliga uppgifter* och definitionen av detta begrepp. Överväganden finns i avsnitt 3.5.1. Bestämmelserna motsvarar 1 kap. 4 § och 5 kap. 1 § andra stycket i 2012 års kustbevakningsdatalag, se vidare a. prop. s. och 192 f. och 221.

16 §

Paragrafen avser en tjänstemans tillgång till personuppgifter. Den motsvarar 2 kap. 3 § i 2012 års lag, se vidare a. prop. s. 198. Överväganden finns i avsnitt 3.5.1. I *andra stycket* har en redaktionell ändring gjorts i förhållande till bestämmelsen i 2012 års lag på så sätt att en hänvisning till 8 kap. 7 § regeringsformen har lagts till.

17 §

Paragrafen upplyser om regeringens möjlighet att föreskriva sekretessbrytande bestämmelser samt om det förhållandet att det redan kan framgå av sekretesslagen att sekretessen kan ge vika i vissa fall. Överväganden finns i avsnitt 3.5.1. Paragrafen motsvarar 5 kap. 6 § i 2012 års kustbevakningsdatalag, se vidare a. prop. s. 224. Den har endast ändrats redaktionellt, se kommentaren till 16 §.

18 §

Paragrafen anger den grundläggande förutsättningen för direktåtkomst för andra myndigheter till personuppgifter som behandlas enligt lagen. Överväganden finns i avsnitt 3.5.1. Bestämmelsen motsvarar 2 kap. 9 § i 2012 års kustbevakningsdatalag, se vidare a. prop. s. 201 f.

19 §

Paragrafen innehåller en reglering av elektroniskt utlämnande av personuppgifter, utom såvitt avser direktåtkomst, som regleras särskilt i 20–23 §§. Med elektroniskt utlämnande avses därmed bl.a. utlämnande genom e-post eller annan elektronisk överföring eller utlämnande på ett usb-minne eller annat motsvarande medium. Överväganden finns i avsnitt 3.5.5.

Bestämmelsen motsvaras av 2 kap. 8 § första stycket kustbevakningens brottsdatalag och är avsedd tillämpas på samma sätt som den bestämmelsen. I författningskommentaren till den bestämmelsen redogörs för vad som ska beaktas vid prövningen om ett elektroniskt utlämnande är olämpligt (SOU 2017:74 s. 907 f.)

20–23 §§

Paragraferna innehåller bestämmelser om direktåtkomst. Överväganden finns i avsnitt 3.5.1. Paragraferna motsvaras av bestämmelserna i 5 kap. 5 § i 2012 års kustbevakningsdatalag, se vidare a. prop. s. 223. Paragrafernas upplysningsbestämmelser har ändrats endast redaktionell, se kommentaren till 16 §.

24 §

I paragrafen finns bestämmelser om information till den registrerade vid insamling av personuppgifter genom bilder eller ljud och i larmsituationer. Överväganden finns i avsnitt 3.5.6.

När det gäller *bild- och ljudupptagningar* finns ett motsvarande undantag i 2 kap. 2 § tredje stycket i 2012 års kustbevakningsdatalag. Det undantaget avser kraven på information enligt personuppgiftslagen. Den förevarande bestämmelsen är avsedd att tillämpas på i princip samma sätt. Det ska dock beaktas att den är en precisering av den princip som finns i artikel 11 i dataskyddsförordningen och tolkas i enlighet därmed. Av förordningens artikel 11.1 följer att om en personuppgiftsansvarig behandlar personuppgifter för ett ändamål som inte kräver att den registrerade identifieras är den personuppgiftsansvarige inte skyldig att bevara, förvärva eller behandla ytterligare information för att identifiera den registrerade endast i syfte att följa förordningen. Om personuppgifter alltså har samlats in genom bilder eller ljud och identifieringen av en person i upptagningarna inte kan göras utan att Kustbevakningen samlar in ytterligare information, enbart i syfte att identifiera honom eller henne, är bestämmelsen tillämplig.

I *larmsituationer* inskränks skyldigheten att lämna information som följer av artikel 13 i dataskyddsförordningen, men endast om det med hänsyn till omständigheterna inte finns tid att lämna sådan information. Bestämmelsen blir endast tillämplig om det annars skulle föreligga en informationsskyldighet. Om insamlingen av personuppgifter i en larmsituation sker genom en ljudupptagning, exempelvis genom inspelning av ett larmsamtal, och personen som ringer inte är direkt identifierbar i enlighet med första stycket, har Kustbevakningen redan p.g.a. detta ingen skyldighet att lämna

information. Bestämmelsen är i övrigt avsedd att tillämpas på samma sätt som motsvarande bestämmelse om information i larmsituationer som finns i 2 kap. 2 § tredje stycket i 2012 års kustbevakningsdatalag, se vidare a. prop. s. 197 f.

25 §

Paragrafen motsvaras av 5 kap. 7 § i 2012 års kustbevakningsdatalag, se vidare a. prop. s. 224 f. Ändringen i paragrafen avser en språklig justering för att paragrafens uttryckssätt ska överensstämma med dataskyddsförordningens terminologi. Överväganden finns i avsnitt 3.5.7. Upplysningsbestämmelserna om föreskriftsrätt har ändrats endast redaktionellt, se kommentaren till 16 §.

Ikraftträdande

Lagen träder i kraft den 25 maj 2018, samtidigt som dataskyddsförordningen ska börja tillämpas.

16.2 Förslaget till lag om ändring i vapenlagen

2 §

Paragrafen är ny. Övervägandena finns i avsnitt 4.1.5.

I paragrafens *första stycke* upplyses om att 1 a kap. vapenlagen innehåller kompletterande bestämmelser till dataskyddsförordningen. Dataskyddsförordningen är direkt tillämplig. Bestämmelserna i 1 a kap. vapenlagen utgör tillåtna preciseringar och kompletteringar i förhållande till dataskyddsförordningens direkt gällande reglering av personuppgiftsbehandling.

I paragrafens *andra stycke* anges att även dataskyddslagen gäller vid behandling av personuppgifter enligt 1 a kap. vapenlagen, om inte kapitlet, eller föreskrifter som meddelats med stöd av det, innehåller avvikande bestämmelser. Avvikande bestämmelser finns i 1 a kap. 3 och 4 §§ som gäller känsliga personuppgifter. Dessa ska alltså tillämpas i stället för regleringen av sådana uppgifter som finns i 3 kap. 3 och 4 §§ dataskyddslagen.

3 §

Paragrafen har ändrats. Överväganden finns i avsnitt 4.1.5.

Paragrafens *första stycke* har ändrats på så sätt att den tidigare uppräknningen av vissa kategorier av personuppgifter har ersatts med en hänvisning till de kategorier som anges i artikel 9.1 i dataskyddsförordningen. Artikeln innehåller dock i huvudsak samma kategorier av personuppgifter som tidigare angavs direkt i lagtexten. Därutöver avser artikel 9.1 biometriska och genetiska uppgifter.

Paragrafens *andra stycke* har endast anpassats språkligt för att utformningen ska överensstämja med regleringen i 2 kap. 11 § brottsdatalagen. Avsikten är att bestämmelserna i andra stycket ska tillämpas på samma sätt som bestämmelserna i 2 kap. 2, 11 och 13 §§ brottsdatalagen, se vidare SOU 2017:29 s. 682 f. och 691 f.

4 §

Paragrafen är ny. Den ersätter dock den tidigare 4 § som hade ett liknande innehåll. Överväganden finns i avsnitt 4.1.5.

Bestämmelsen innehåller sökbegränsningar avseende känsliga personuppgifter. Den är utformad i enlighet med sökbegränsningen i 2 kap. 14 § brottsdatalagen och är avsedd att tillämpas på motsvarande sätt, se vidare SOU 2017:29 s. 693.

Ikraftträdande

Lagen träder i kraft den 25 maj 2018, samtidigt som dataskyddsförordningen ska börja tillämpas.

16.3 Förslaget till lag om ändring i lagen om belastningsregister

1 a §

Paragrafen har i huvudsak ett nytt innehåll. Överväganden finns i avsnitt 5.5.

Första stycket innehåller en upplysning om att lagen gäller utöver brottsdatalagen, i stället för som tidigare utöver personuppgifts-

lagen (1998:204). Innebörden av att lagen gäller utöver brottsdatalagen är densamma som att den tidigare gällde utöver personuppgiftslagen. Innebörden är också densamma som motsvarande bestämmelser i andra registerlagar inom brottsdatalagens tillämpningsområde, jfr exempelvis 1 kap. 1 § polisens brottsdatalag och kommentaren till denna (SOU 2017:74 s. 866). Det innebär att brottsdatalagen tillämpas avseende frågor som inte regleras särskilt i lagen om belastningsregister.

För förändret av belastningsregistret, dvs. införande av uppgifter och bevarande i registret till dess uppgifterna ska gallras enligt bestämmelserna i 16–18 §§, utgör alltså lagen om belastningsregister ett komplement till brottsdatalagen. Detta innebär att exempelvis frågor om säkerhet för registret, tillsyn, rättelse m.fl. frågor som har med registrets innehåll att göra och som inte regleras i lagen om belastningsregister, regleras av brottsdatalagen. När uppgifter behandlas i registret för att användas för sådana ändamål som anges i 2 § första stycket 1–3 är också brottsdatalagen tillämplig. Vissa uttag enligt 2 § första stycket 4 omfattas också av brottsdatalagens tillämpningsområde. Det rör framför allt prövningar av olika frågor som har samband med verkställighet av straff som görs av behöriga myndigheter, exempelvis frågor om utlämning för brott, ärenden om nåd, frågor enligt fängelselagen (2010:610) eller häkteslagen (2010:611) eller frågor om övervakning. I avsnitt 5.2 finns en utförligare genomgång.

Behandling i registret för sådana ändamål som anges i 2 § 1–3 är inte en behandling för nya ändamål enligt 2 kap. 4 § brottsdatalagen. Den paragrafens proportionalitetsbedömning behöver alltså inte utföras.

I *andra stycket* görs ett undantag från sökbegränsningen i brottsdatalagen. Det innebär att brottsrubriceringar och uppgifter om påföljd och verkställighet av påföljd får användas som sökbegrepp, även om detta skulle kunna innebära att en sammanställning som innehåller känsliga personuppgifter tas fram. Bestämmelsen motsvaras delvis av 2 kap. 5 § polisens brottsdatalag. I de delar bestämmelsen överensstämmer med bestämmelsen i polisens brottsdatalag är den avsedd att tillämpas på motsvarande sätt. Se vidare kommentaren till polisens brottsdatalag, SOU 2017:74 s. 872 f.

1 b §

Paragrafen är ny. Överväganden finns i avsnitt 5.5.

I paragrafens upplyses om det förhållandet att dataskyddsförordningen gäller för behandling i registret som görs för andra syften än sådana som omfattas av brottsdatalagens tillämpningsområde. Därtill gäller dataskyddslagen för sådan behandling, vilket också framgår.

Behandlingar i registret som inte omfattas av brottsdatalagens tillämpningsområde är i huvudsak utlämnande av uppgifter ur registret för sådana tillstånds- och lämplighetsprövningar som avses i 2 § första stycket 4, exempelvis sådana prövningar som f.n. tas upp i 11–18 §§ förordningen om belastningsregister. En närmare redogörelse finns i avsnitt 5.2. Även Polismyndighetens egen användning av registret för lämplighetsprövningar m.m. som inte omfattas av Polismyndighetens uppdrag som behörig myndighet, i enlighet med brottsdatalagen, omfattas av dataskyddsförordningens tillämpningsområde.

2 §

Paragrafen har ändrats i *första stycket 1*. Överväganden finns i avsnitt 5.5. Ändringen innebär att uttryckssättet har anpassats till 1 kap. 2 § brottsdatalagen (och 2 kap. 1 §) som beskriver de syften som avgränsar brottsdatalagens tillämpningsområde (respektive definierar den rättsliga grunden för behandling av personuppgifter). Ändringen avser inte någon egentlig förändring i sak. Vad som avses med de uppräknade ändamålen ska dock förstås på samma sätt som i brottsdatalagen. Ändringen skulle därmed kunna innebära en viss utvidgning, beroende på den närmare innebörd som kan framkomma vid tillämpningen av bestämmelserna i brottsdatalagen.

9 §

Paragrafens *första stycke* har ändrats så att den registrerades rätt att få ett fullständigt registerutdrag har utgått. I första stycket finns i stället en upplysning om att rätten till information om behandling

av personuppgifter finns i 4 kap. 3 § brottsdatalagen. En enskild som önskar ett utdrag avseende sig själv kan alltså begära information enligt det nämnda lagrummet. Någon skillnad i sak för den enskildes rätt att kunna få ett fullständigt utdrag om sina egna belastningsuppgifter är inte avsedd. Överväganden finns i avsnitt 5.5.

Paragrafen är oförändrad när det gäller den registrerades möjligheter att få begränsade registerutdrag för vissa specifika syften (andra stycket). Även tredje stycket är oförändrat. En registrerad som begär ett begränsat registerutdrag ska göra en *skriftlig begäran*. I detta avseende är det heller ingen skillnad mot tidigare bestämmelser. Paragrafens *fjärde stycke* har dock ändrats så att det utöver en skriftlig begäran i pappersform ska vara möjligt att ge in en begäran i olika former av elektroniska dokument, om Polismyndigheten kan säkerställa att begäran görs av en behörig person. Bestämmelsen motsvaras av 4 kap. 2 § i brottsdataförordningen och avsikten är att den ska tillämpas på samma sätt. Se vidare SOU 2017:29 s. 413.

20 §

Paragrafen har fått ett delvis nytt innehåll. Överväganden finns i avsnitt 5.5.

I stället för en hänvisning till skadeståndsregleringen i personuppgiftslagen görs en hänvisning till brottsdatalagen, med avseende på skadestånd som omfattas av brottsdatalagens tillämpningsområde. Skadestånd med anledning av behandlingar som omfattas av dataskyddsförordningens tillämpningsområde regleras direkt i dataskyddsförordningen.

Ikraftträdande och övergångsbestämmelser

Ändringarna i lagen om belastningsregister träder i huvudsak i kraft den 1 maj 2018, samma dag som brottsdatalagen. Det gäller även upphävandet av 1 b §. Införandet av den nya 1 b § i lagen träder dock i kraft den 25 maj 2018, samma dag som dataskyddsförordningen börjar tillämpas.

För behandling som inte omfattas av brottsdatalagens tillämpningsområde ska lagen om belastningsregister i sin lydelse före den 1 maj 2018 fortsätta att tillämpas fram till den 25 maj 2018. Det innebär att för sådan behandling gäller, fram till den 25 maj 2018, personuppgiftslagens bestämmelser, bl.a. om rättelse och skadestånd. Vilken behandling som omfattas av brottsdatalagens respektive dataskyddsförordningens tillämpningsområde har utvecklats i kommentaren till 1 a och 1 b §§ och har även övervägts i avsnitt 5.2.

16.4 Förslaget till lag om ändring i lagen om misstankeregister

1 a § och 15 §§

Paragraferna har fått ett nytt innehåll. Överväganden finns i avsnitt 6.5. Ändringarna i paragraferna motsvaras i stort av ändringarna i 1 a § och 20 § lagen om belastningsregister. I 1 a § andra stycket anges dock endast brottsrubriceringar som tillåtna sökbegrepp (jfr 1 a § lagen om belastningsregister som också tar upp *verkställighet av påföljd* som ett tillåtet sökbegrepp, eftersom belastningsregistret, till skillnad från misstankeregistret, innehåller den typen av uppgifter). Se vidare kommentaren till ändringarna i lagen om belastningsregister i föregående avsnitt, avsnitt 16.3.

1 b §

Paragrafen är ny. Överväganden finns i avsnitt 6.5. Paragrafens innehåll är detsamma som innehållet i 1 b § lagen om belastningsregister. Se vidare kommentaren till den paragrafen i föregående avsnitt, avsnitt 16.3).

2 §

Paragrafen har ändrats i *första stycket 1*. Överväganden finns i avsnitt 6.5. Ändringen motsvarar ändringen i 2 § första stycket 1 lagen om belastningsregister och är avsedd att ha samma innebörd som i den bestämmelsen. Se vidare kommentaren till 2 § lagen om belastningsregister i föregående avsnitt, avsnitt 16.3.

8 §

Paragrafen har ändrats i *andra stycket*. Överväganden finns i avsnitt 6.5. Ändringen överensstämmer i sak med den ändring som gjorts i 9 § fjärde stycket lagen om belastningsregister. Se vidare kommentaren till den ändringen i föregående avsnitt, avsnitt 16.3.

Ikraftträdande och övergångsbestämmelser

Bestämmelserna har samma innehåll och innebörd som motsvarande bestämmelser i lagen om belastningsregister, se vidare avsnitt 16.3.

16.5 Förslaget till lag om ändring i lagen om Schengens informationssystem

1 a §

Paragrafen är ny. Överväganden finns i avsnitt 7.4.

I paragrafens *första stycke* anges att lagen om Schengens informationssystem (SIS) gäller utöver brottsdatalagen. Innebörden är densamma som motsvarande bestämmelser i andra registerlagar inom brottsdatalagens tillämpningsområde, jfr exempelvis 1 kap. 1 § polisens brottsdatalag och kommentaren till denna (SOU 2017:74 s. 866). Brottsdatalagen tillämpas alltså avseende frågor som inte regleras särskilt i lagen om SIS med avseende på sådan personuppgiftsbehandling i registret som sker för de syften som avgränsar brottsdatalagens tillämpningsområde.

Av paragrafens *andra stycke* följer att lagen om SIS i vissa avseenden innehåller avvikande bestämmelser i förhållande till brottsdatalagen. Regleringen i SIS gäller därmed i stället för de uppräknade bestämmelserna i brottsdatalagen. Således gäller enligt 10 § första stycket lagen om SIS ett förbud mot överföringar till tredje land och internationella organisationer, vilket innebär att 7 kap. brottsdatalagen inte är tillämpligt. Möjligheten att vidarebehandla uppgifter ur SIS eller viss tilläggsinformation är vidare begränsad i 10 och 13 §§ i lagen och någon vidarebehandling med stöd av 2 kap. 4 eller 22 §§ brottsdatalagen kan inte vidtas. Slutligen

regleras användningen av känsliga personuppgifter i SIS uttömmande i lagen. Någon behandling av sådana uppgifter med stöd av 2 kap. 11 § brottsdatalagen är inte tillåten.

1 b §

Paragrafen är ny. Överväganden finns i avsnitt 7.4.

Bestämmelsen upplyser i *första stycket* om att det finns bestämmelser om personuppgiftsbehandling i dataskyddsförordningen och dataskyddslagen. Det gäller sådan behandling av personuppgifter som inte omfattas av brottsdatalagens tillämpningsområde. Det rör sig i huvudsak om efterlysningar av personer som inte har med bekämpandet av brott att göra, exempelvis personer som ska omhändertas p.g.a. beslut om tvångsvård (jfr de grunder för registrering i SIS som tas upp i 5 § i förordningen om SIS).

I *andra stycket* anges att den särskilda regleringen av känsliga personuppgifter i SIS avviker från 3 kap. 3 och 4 §§ dataskyddslagen. I stället gäller för de flesta känsliga personuppgifter, nämligen sådana som räknas upp i 7 §, att det inte är tillåtet att föra in sådana uppgifter i SIS. När det däremot gäller fingeravtryck, som också räknas in i kategorin känsliga personuppgifter enligt dataskyddslagen, innebär regleringen i lagen om SIS att behandling av sådana personuppgifter är tillåten.

16 §

Paragrafen har ändrats. Överväganden finns i avsnitt 7.4.

Ändringarna överensstämmer med ändringarna i 20 § lagen om belastningsregister och 15 § lagen om misstankeregister, se vidare kommentaren till 20 § i lagen om belastningsregister, avsnitt 16.3.

Ikraftträdande och övergångsbestämmelser

Bestämmelserna har samma innehåll och innebörd som motsvarande bestämmelser i lagen om belastningsregister, se vidare avsnitt 16.3.



REGERINGSKANSLIET

Promemoria

2016-10-12

Justitiedepartementet

*Enheten för lagstiftning om allmän ordning och säkerhet
och samhällets krisberedskap (L4)*

Anna Westin

Telefon 08-405 48 78

Mobil 070-357 88 21

E-post anna.westin@regeringskansliet.se

EU:s dataskyddsreform – anpassningar av författningar om allmän ordning och säkerhet och samhällets krisberedskap

Bakgrund

Inom EU har det antagits en ny reglering av skyddet för enskilda vid behandling av personuppgifter. Den består av två rättsliga instrument, en förordning och ett direktiv.

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 (dataskyddsförordningen) börjar tillämpas den 25 maj 2018. Förordningen utgör en ny generell reglering för behandling av personuppgifter inom EU och kommer att ersätta dataskyddsdirektivet från år 1995. Det innebär bl.a. att personuppgiftslagen (1998:204) måste upphävas. Förordningen baseras till stor del på dataskyddsdirektivets struktur och innehåll men innebär även en rad nyheter såsom en utökad informationsskyldighet och inrättandet av Europeiska dataskyddsstyrelsen. Dataskyddsförordningen är direkt tillämplig i medlemsstaterna men både förutsätter och möjliggör kompletterande nationella bestämmelser av olika slag.

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 (det nya dataskyddsdirektivet) ska vara genomfört i nationell rätt senast den 6 maj 2018. Personuppgiftsbehandling som faller under direktivets tillämpningsområde är undantagen från dataskyddsförordningens tillämpningsområde.

Dataskyddsförordningen och det nya dataskyddsdirektivet kräver en bred översyn av författningarna om personuppgiftsbehandling. Bland

pågående utredningsarbete bör nämnas att en särskild utredare har i uppdrag att föreslå de anpassningar och kompletterande författningsbestämmelser på generell nivå som dataskyddsförordningen ger anledning till (dir. 2016:15). Den utredningen, som tagit sig namnet Dataskyddsutredningen, har i uppdrag att säkerställa att det finns en ändamålsenlig och välbalanserad kompletterande nationell reglering om personuppgiftsbehandling när förordningen börjar tillämpas. En annan särskild utredare har i uppdrag att föreslå hur det nya dataskyddsdirektivet ska genomföras i svensk rätt (dir. 2016:21). Den utredningen, som tagit sig namnet Utredningen om 2016 års dataskyddsdirektiv, ska bl.a. lämna förslag till en ny ramlagstiftning med bestämmelser om skydd av personuppgifter inom direktivets tillämpningsområde.

Behovet av en utredning

Enheten för lagstiftning om allmän ordning och säkerhet och samhällets krisberedskap vid Justitiedepartementet (Enheten) ansvarar för ett flertal författningar som i större eller mindre utsträckning reglerar personuppgiftsbehandling. Vissa av dem är renodlade s.k. registerförfattningar medan andra endast innehåller ett fåtal bestämmelser som rör personuppgiftsbehandling. Exempelvis kan följande författningar nämnas: lagen (1998:620) om belastningsregister, lagen (1998:621) om misstankeregister, vapenlagen (1996:67), säkerhetsskyddslagen (1996:627), förordningen (2015:476) om behandling av personuppgifter i Nationellt forensiskt centrum's uppdragsverksamhet, förordningen (1967:502) om utdrag ur folkbokföringsdatabasen i och för utredning angående brott m.m., förordningen (1958:272) om tjänstekort och efterlysningsskugörelsen (1969:293).

Dataskyddsutredningens uppdrag omfattar inte att se över sådan sektorspecifik reglering om behandling av personuppgifter som bl.a. finns i de särskilda registerförfattningarna. Utredningen om 2016 års dataskyddsdirektiv ska anpassa vissa centrala författningar som reglerar rättsväsendets behandling av personuppgifter, bl.a. polisdatalagen och de bestämmelser i kustbevakningsdatalagen som rör brottsbekämpning, till de nya förutsättningarna, men har inte i uppdrag att se över alla författningar som berörs av det nya dataskyddsdirektivet. Mot denna bakgrund finns det behov av att utreda vilka författningsändringar EU:s dataskyddsreform föranleder i fråga om den personuppgiftsreglering som Enheten ansvarar för, men som inte omfattas av de ovan nämnda utredningarnas uppdrag.

Det avgörande för om en viss personuppgiftsbehandling kommer att omfattas av dataskyddsförordningen eller det nya dataskyddsdirektivet kommer att vara i vilket syfte uppgifterna behandlas. Myndigheter vars kärnverksamhet huvudsakligen omfattas av det nya dataskyddsdirektivets tillämpningsområde kommer att tillämpa dataskyddsförordningen

när personuppgifter behandlas i annan verksamhet och när de i den brottsbekämpande verksamheten t.ex. överför uppgifter för ändamål utanför direktivets tillämpningsområde. En utredning behöver därför analysera både dataskyddsförordningen och dataskyddsdirektivet i förhållande till de författningar som Enheten ansvarar för men som inte omfattas av de uppdrag som Dataskyddsutredningen eller Utredningen om 2016 års dataskyddsdirektiv har.

Uppdraget

En utredare ges i uppdrag att undersöka vilka anpassningar som är behövliga eller lämpliga och lämna förslag på de författningsändringar som EU:s dataskyddsreform föranleder i fråga om den personuppgiftsreglering som Enheten ansvarar för, och som inte tas om hand av Dataskyddsutredningen eller Utredningen om 2016 års dataskyddsdirektiv.

Utredaren är även fri att ta upp och lämna förslag i näraliggande frågor som aktualiseras under utredningsuppdraget men som inte rör genomförandet av eller anpassningen av svensk rätt till EU:s dataskyddsreform.

Utredaren ska analysera och redovisa förslagets ekonomiska konsekvenser. Om kostnader bedöms uppkomma ska ett finansieringsförslag lämnas. Utredaren ska också redovisa förslagets konsekvenser för den personliga integriteten samt för brottsbekämpningen och övrig berörd verksamhet.

Under utförandet av uppdraget ska utredaren samråda med Utredningen om 2016 års dataskyddsdirektiv och informera sig om annat pågående utredningsarbete som kan vara av betydelse för uppdragets genomförande. Utredaren ska också, i den utsträckning som bedöms lämplig, inhämta synpunkter och upplysningar från Polismyndigheten och andra myndigheter som kan vara berörda av aktuella frågor.

Uppdraget ska redovisas senast den 19 november 2017.

Departementsserien 2017

Kronologisk förteckning

1. Elektronisk övervakning av kontaktförbud. Ju.
2. Åldersdifferentierat underhållsstöd och höjt grundavdrag för bidragsskyldiga föräldrar. S.
3. Genomförande av ICT-direktivet. Ju.
4. Sjukpenning i avvaktan på slutligt beslut. S.
5. Effektivare sanktioner i livsmedelskedjan m.m. N.
6. Förslag till lag om ersättning till personer som har fått ändrad könstillhörighet fastställd i vissa fall. S.
7. Kommunikation för vår gemensamma säkerhet. Uppdrag om en utvecklad och säker kommunikationslösning för aktörer inom allmän ordning, säkerhet, hälsa och försvar. Ju.
8. Kultursamverkan för ett Sverige som håller ihop. Framtida inriktning och utvecklingsmöjligheter för kultursamverkansmodellen. Ku.
9. Förstärkt rehabilitering för återgång i arbete. S.
10. ILO:s konvention om anständiga arbetsvillkor för hushållsarbetare. A.
11. Ändrade regler om retroaktivitet avseende efterlevandestöd. S.
12. Om förenklat beslutsfattande och särskilda boendeformer för äldre. S.
13. Skadeståndets bestämmande vid finansiell rådgivning. Fi.
14. Vissa ändringar i läkemedelslagen. S.
15. Ökat konsulärt skydd för unionsmedborgare och deras familjemedlemmar. Genomförande av direktiv (EU) 2015/637. UD.
16. Arbetsplatsinspektioner och höjd särskild avgift. Ju.
17. En ny lag om försäkringsdistribution. Fi.
18. Karensavdrag – en mer rättvis självrisk. S.
19. Anpassningar av de fastighetsrättsliga, associationsrättsliga, transporträttsliga och immaterialrättsliga författningarna till dataskyddsförordningen. Ju.
20. Regionalt utvecklingsansvar i Stockholms, Kalmar och Blekinge län. Fi.
21. Skyldighet för vissa offentliga funktionärer att anmäla innehav av finansiella instrument. Fi.
22. Utstationering och vägtransporter. A.
23. Kompletterande bestämmelser till EU:s förordning om personlig skyddsutrustning. Fi.
24. Skjutvapen och explosiva varor – Skärpta straff för de grova brotten. Ju.
25. Nya ungdomspåföljder. Ju.
26. En anpassning till dataskyddsförordningen – kreditupplysningslagen och några andra författningar. Ju.
27. Genomförande av säsongsanställningsdirektivet. Ju.
28. En anpassning till dataskyddsförordningen av dataskyddsbestämmelser inom Näringsdepartementets verksamhetsområde. N.
29. Utökade möjligheter till utbyte av läkemedel. S.
30. Ett entreprenörsansvar i bygg- och anläggningsbranschen. A.
31. Elektroniska fakturor vid offentlig upphandling. Fi.
32. Biologiskt mångfald och ekosystemtjänster. Kontrollstation 2016. M.
33. Anpassningar till dataskyddsförordningen av registerförfattningar inom Arbetsmarknadsdepartementets ansvarsområde. A.
34. Ändringar i bestämmelser om val till Sametinget. K.
35. Körkortslån. A.
36. En snabbare lagföring. Försöksprojekt med ett snabbförfarande i brottmål. Ju.

37. Frekventa och omfattande ärenden om utlämnande av allmän handling. Ju.
38. Livstidsstraff för mord. Ju.
39. Legitimation för hälso- och sjukvårdskuratorer. S.
40. Ändringar i vissa författningar inom Finansdepartementets ansvarsområde med anledning av EU:s dataskyddsreform. Fi.
41. En omarbetad domstolsdatalag. Anpassning till EU:s dataskyddsförordning. Ju.
42. Följdändringar till ny förvaltningslag. Ju.
43. Konsultation i frågor som rör det samiska folket. Ku.
44. Elmarknadslag. M.
45. En omarbetad utlänningsdatalag. Anpassning till EU:s dataskyddsförordning. Ju.
46. Kriminalvårdens datalag. Anpassning till EU:s dataskyddsförordning. Ju.
47. Utredningar avseende vissa skador och dödsfall. S.
48. Statistik på upphandlingsområdet. Fi.
49. Omedelbart omhändertagande av barn och unga i vissa internationella situationer. S.
50. Ett moderniserat medinflytande för totalförsvarspliktiga. Fö.
51. Sweden's sixth national report under the Joint Convention on the safety of spent fuel management and on the safety of radioactive waste management. M.
52. Tillgång till upphovsrättsligt skyddat material för personer med läsnedsättning. Ju.
53. Rätten till offentlig försvarare. Genomförande av EU:s rättshjälpsdirektiv. Ju.
54. En anpassning till dataskyddsförordningen av författningar inom Miljö- och energidepartementets verksamhetsområde. M.
55. En karensdag mindre i arbetslöshetsförsäkringen. A.
56. Bastjänstgöring för läkare. S.
57. Följdändringar till ändrade mediegrundlag. Ju.
58. EU:s dataskyddsreform – anpassningar av vissa författningar om allmän ordning och säkerhet. Ju.

Departementsserien 2017

Systematisk förteckning

Arbetsmarknadsdepartementet

- ILO:s konvention om anständiga arbetsvillkor för hushållsarbetare. [10]
- Utstationering och vägtransporter. [22]
- Ett entreprenörsansvar i bygg- och anläggningsbranschen. [30]
- Anpassningar till dataskyddsförordningen av registerförfattningar inom Arbetsmarknadsdepartementets ansvarsområde. [33]
- Körkortslån. [35]
- En karensdag mindre i arbetslöshetsförsäkringen. [55]

Finansdepartementet

- Skadeståndets bestämmande vid finansiell rådgivning. [13]
- En ny lag om försäkringsdistribution. [17]
- Regionalt utvecklingsansvar i Stockholms, Kalmar och Blekinge län. [20]
- Skyldighet för vissa offentliga funktionärer att anmäla innehav av finansiella instrument. [21]
- Kompletterande bestämmelser till EU:s förordning om personlig skyddsutrustning. [23]
- Elektroniska fakturor vid offentlig upphandling. [31]
- Ändringar i vissa författningar inom Finansdepartementets ansvarsområde med anledning av EU:s dataskyddsreform. [40]
- Statistik på upphandlingsområdet. [48]

Försvarsdepartementet

- Ett moderniserat medinflytande för totalförsvarspiktiga. [50]

Justitiedepartementet

- Elektronisk övervakning av kontaktförbud. [1]

- Genomförande av ICT-direktivet. [3]
- Kommunikation för vår gemensamma säkerhet. Uppdrag om en utvecklad och säker kommunikationslösning för aktörer inom allmän ordning, säkerhet, hälsa och försvar. [7]
- Arbetsplatsinspektioner och höjd särskild avgift. [16]
- Anpassningar av de fastighetsrättsliga, associationsrättsliga, transporträttsliga och immaterialrättsliga författningarna till dataskyddsförordningen. [19]
- Skjutvapen och explosiva varor – Skärpta straff för de grova brotten. [24]
- Nya ungdomspåföljder. [25]
- En anpassning till dataskyddsförordningen – kreditupplysningslagen och några andra författningar. [26]
- Genomförande av säsongsanställningsdirektivet. [27]
- En snabbare lagföring. Försöksprojekt med ett snabbförfarande i brottmål. [36]
- Frekventa och omfattande ärenden om utlämnande av allmän handling. [37]
- Livstidsstraff för mord. [38]
- En omarbetad domstolsdatalog. Anpassning till EU:s dataskyddsförordning. [41]
- Följdändringar till ny förvaltningslag. [42]
- En omarbetad utlämningsdatalog. Anpassning till EU:s dataskyddsförordning. [45]
- Kriminalvårdens datalog. Anpassning till EU:s dataskyddsförordning. [46]
- Tillgång till upphovsrättsligt skyddat material för personer med läsnedsättning. [52]
- Rätten till offentlig försvare. Genomförande av EU:s rättshjälpsdirektiv. [53]
- Följdändringar till ändrade mediegrundlagar. [57]

EU:s dataskyddsreform – anpassningar av vissa författningar om allmän ordning och säkerhet. [58]

Kulturdepartementet

Kultursamverkan för ett Sverige som håller ihop. Framtida inriktning och utvecklingsmöjligheter för kultursamverkansmodellen. [8]

Ändringar i bestämmelser om val till Sametinget. [34]

Konsultation i frågor som rör det samiska folket. [43]

Miljö- och energidepartementet

Biologisk mångfald och ekosystemtjänster. Kontrollstation 2016. [32]

Elmarknadslag. [44]

Sweden's sixth national report under the Joint Convention on the safety of spent fuel management and on the safety of radioactive waste management. [51]

En anpassning till dataskyddsförordningen av författningar inom Miljö- och energidepartementets verksamhetsområde. [54]

Näringsdepartementet

Effektivare sanktioner i livsmedelskedjan m.m. [5]

En anpassning till dataskyddsförordningen av dataskyddsbestämmelser inom Näringsdepartementets verksamhetsområde. [28]

Socialdepartementet

Åldersdifferentierat underhållsstöd och höjt grundavdrag för bidragsskyldiga föräldrar. [2]

Sjukpenning i avvaktan på slutligt beslut. [4]

Förslag till lag om ersättning till personer som har fått ändrad könstillhörighet fastställd i vissa fall. [6]

Förstärkt rehabilitering för återgång i arbete. [9]

Ändrade regler om retroaktivitet avseende efterlevandestöd. [11]

Om förenklat beslutsfattande och särskilda boendeformer för äldre. [12]

Vissa ändringar i läkemedelslagen. [14]

Karensavdrag – en mer rättvis självrisk. [18]

Utökade möjligheter till utbyte av läkemedel. [29]

Legitimation för hälso- och sjukvårdskuratorer. [39]

Utredningar avseende vissa skador och dödsfall. [47]

Omdelbart omhändertagande av barn och unga i vissa internationella situationer. [49]

Bastjänstgöring för läkare. [56]

Utrikesdepartementet

Ökat konsulärt skydd för unionsmedborgare och deras familjemedlemmar. Genomförande av direktiv (EU) 2015/637. [15]